Round-Optimal
Oblivious Transfer and MPC from Computational CSIDH

Pratik Sarkar (Boston University)

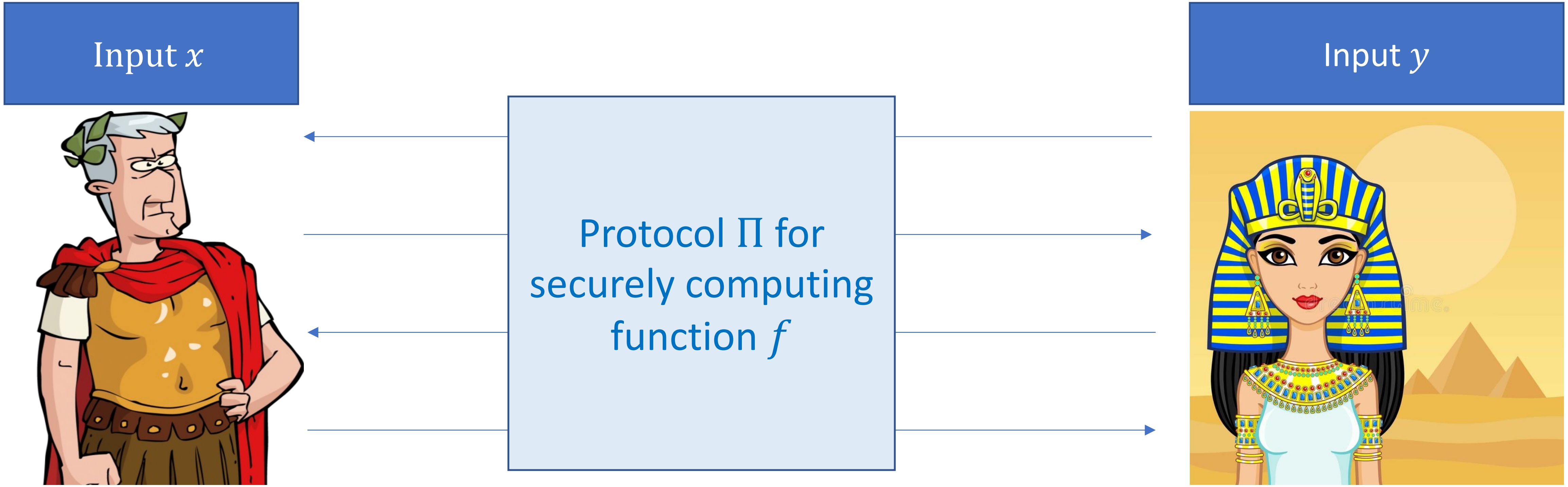
Joint work with

Saikrishna Badrinarayanan, LinkedIn
Daniel Masny, Meta
Pratyay Mukherjee, Supra
Sikhar Patranabis, IBM Research India
Srinivasan Raghuraman, Visa Research

Chapter I

Introduction

Secure Two-Party Computation (2-PC)



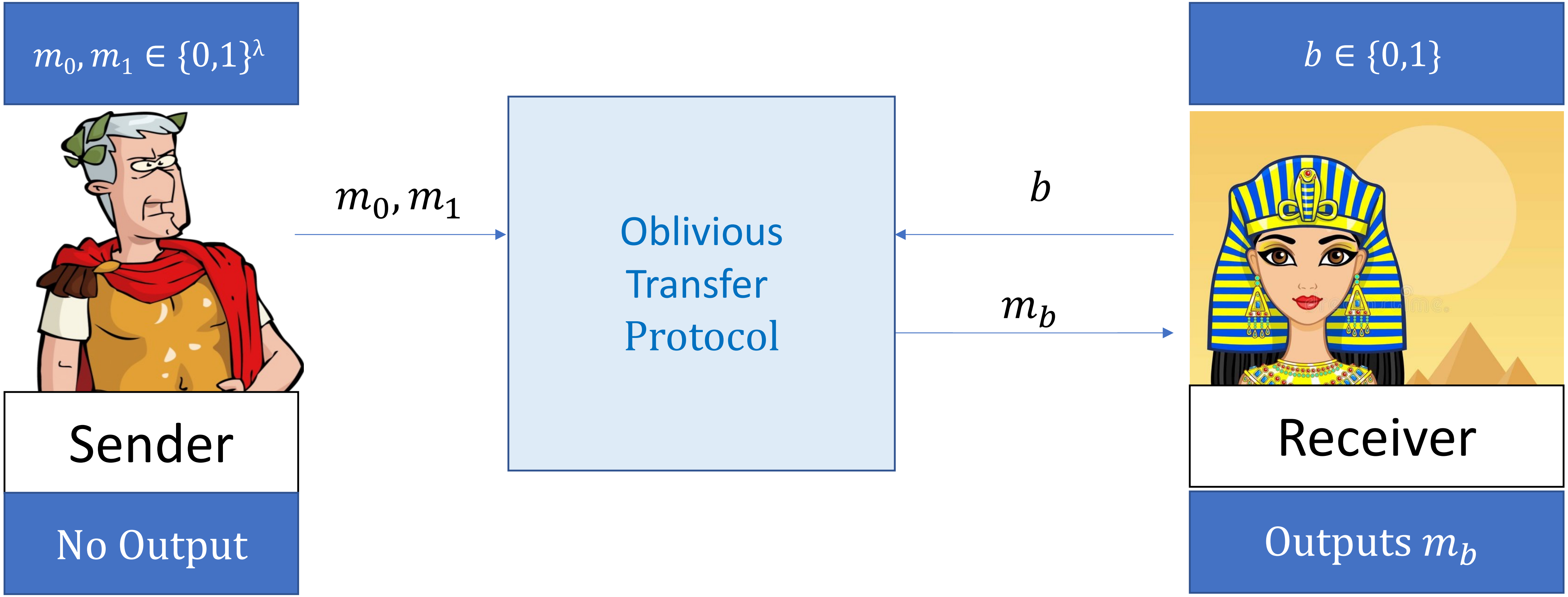
Input x

Protocol Π for securely computing function f

Input y

- Correctness: $\Pi(x, y) = f(x, y)$
- Security: Π leaks no information about x and y beyond $\Pi(x, y)$

Oblivious Transfer (OT)



$m_0, m_1 \in \{0,1\}^\lambda$

Sender

No Output

m_0, m_1

Oblivious Transfer Protocol

b

m_b

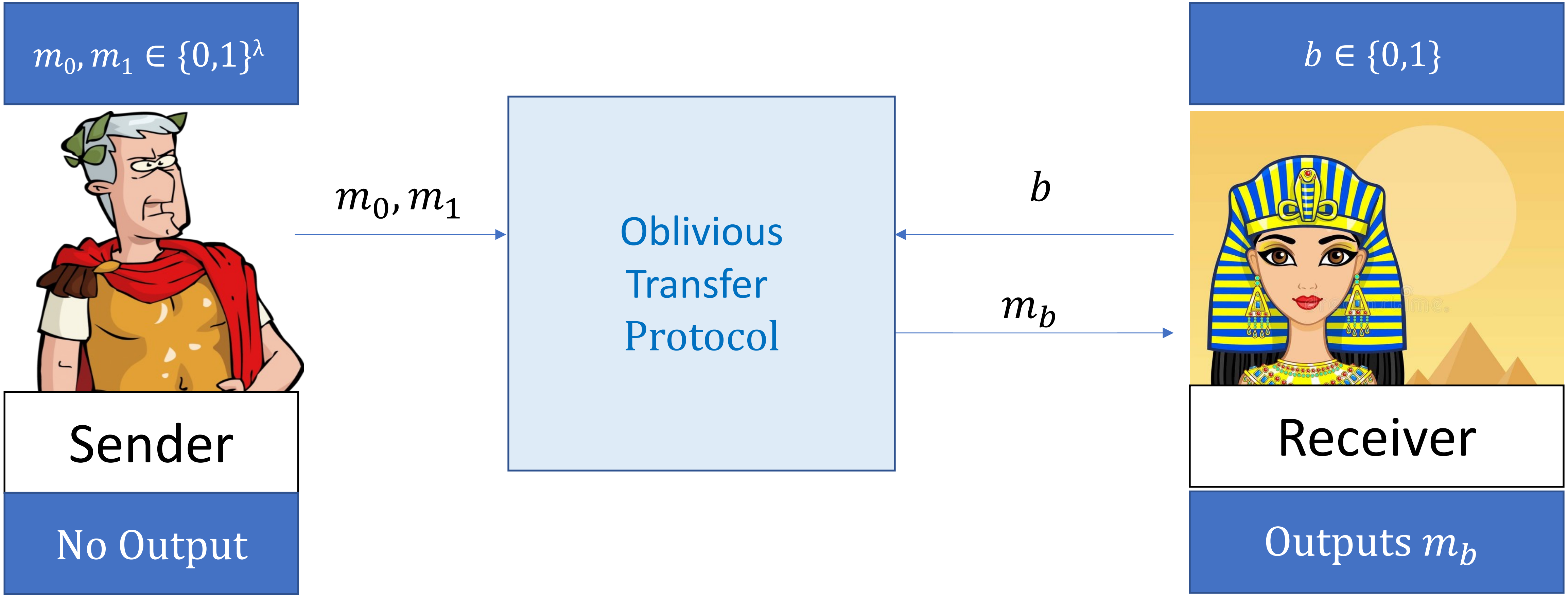
$b \in \{0,1\}$

Receiver

Outputs m_b

Security: Sender does not know b and Receiver does not know m_{1-b}

Oblivious Transfer (OT)



$m_0, m_1 \in \{0,1\}^\lambda$

Sender

No Output

m_0, m_1

Oblivious Transfer Protocol

b

m_b

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

Receiver

Outputs m_b

Security: Sender does not know b and Receiver does not know m_{1-b}

Round-Optimal OT → Round-Optimal MPC [GS18,BL18]

This Talk

Our Focus

OT Protocols in Setup Model and Plain Model:

- Round-Optimal

This Talk

Our Focus

OT Protocols in Setup Model and Plain Model:

- Round-Optimal
- Simulation-Security

This Talk

Our Focus

OT Protocols in Setup Model and Plain Model:

- Round-Optimal
- Simulation-Security
- Weak isogeny-based assumptions

This Talk

Our Focus

OT Protocols in Setup Model and Plain Model:

- Round-Optimal
- Simulation-Security
- Weak isogeny-based assumptions

[BL18,GS18]: MPC in Setup Model and Plain Model:

- Round-Optimal
- Simulation-Security
- Weak isogeny-based assumptions

Chapter II

Contributions and Comparison

Isogeny-based OT Protocols in the Setup Model

Protocol	**Computational Assumptions**	**Rounds**	**Security Model**	**Setup**
[ADMP20]	Decisional CSIDH	2	UC-security	CRS
[BKW20]	Decisional CSIDH	2	UC-security	CRS+Random Oracle
[AMPS21]	Decisional CSIDH	2	UC-security (Adaptive)	CRS
[LGdSG21]	Reciprocal CSIDH	4	UC-security	CRS+Random Oracle
[OZ23]	DLog CSIDH (Knowledge of Exponent)	2	Relaxed UC-security	CRS+Random Oracle

Isogeny-based OT Protocols in the Setup Model

Protocol	Computational Assumptions	Rounds	Security Model	Setup
[ADMP20]	Decisional CSIDH	2	UC-security	CRS
[BKW20]	Decisional CSIDH	2	UC-security	CRS+Random Oracle
[AMPS21]	Decisional CSIDH	2	UC-security (Adaptive)	CRS
[LGdSG21]	Reciprocal CSIDH	4	UC-security	CRS+Random Oracle
[OZ23]	DLog CSIDH (Knowledge of Exponent)	2	Relaxed UC-security	CRS+Random Oracle
This Work	**Computational CSIDH**	**2**	**Simulation security**	**CRS+Random Oracle**

Our Contributions

Round Optimal Results in Setup Model:

- 2-round UC-OT in CRS+Random Oracle Model from computational-CSIDH

Our Contributions

Round Optimal Results in Setup Model:

- 2-round UC-OT in CRS+Random Oracle Model from computational-CSIDH
- 2-round MPC in CRS+Random Oracle Model from computational-CSIDH

Isogeny-based OT Protocols in the Plain Model

Protocol	**Computational Assumptions**	**Rounds**	**Security Model**
[ADMP20]	Decisional CSIDH	2	Semantic security
[BPS22]	Reciprocal CSIDH	4	Simulation security
[KM20]	Decisional CSIDH	4	Simulation security

Isogeny-based OT Protocols in the Plain Model

Protocol	**Computational Assumptions**	**Rounds**	**Security Model**
[ADMP20]	Decisional CSIDH	2	Semantic security
[BPS22]	Reciprocal CSIDH	4	Simulation security
[KM20]	Decisional CSIDH	4	Simulation security
This Work	**Computational CSIDH**	**4**	**Simulation security**

Our Contributions

Round Optimal Results in Setup Model:

- 2-round UC-OT in CRS+Random Oracle Model from computational-CSIDH
- 2-round MPC in CRS+Random Oracle Model from computational-CSIDH

Round Optimal Results in Plain Model:

- 4-round simulation-secure OT without Setup from computational-CSIDH

Our Contributions

Round Optimal Results in Setup Model:

- 2-round UC-OT in CRS+Random Oracle Model from computational-CSIDH
- 2-round MPC in CRS+Random Oracle Model from computational-CSIDH

Round Optimal Results in Plain Model:

- 4-round simulation-secure OT without Setup from computational-CSIDH
- 4-round simulation-secure MPC without Setup from computational-CSIDH

Our Contributions

Round Optimal Results in Setup Model:

- 2-round UC-OT in CRS+Random Oracle Model from computational-CSIDH
- 2-round MPC in CRS+Random Oracle Model from computational-CSIDH

Round Optimal Results in Plain Model:

- 4-round simulation-secure OT without Setup from computational-CSIDH
- 4-round simulation-secure MPC without Setup from computational-CSIDH

Other Results:

- Oblivious Transfer Extension: Each base-OT requires 4 isogeny computations
- Security based on Reciprocal-CSIDH (quantum equivalent to computational-CSIDH)

Chapter III

Isogeny Preliminaries

Group Actions – Basic Definitions

Definition

Group Action of a group $(G,\cdot)$ on a set $\mathcal{X}$ is a function $* : G \times \mathcal{X} \to \mathcal{X}$ such that:

- Letting e be the identity element in G, for every $x \in \mathcal{X}$ we have $e * x = x$
- For every $g, h \in G$ and for every $x \in \mathcal{X}$ we have $(g \cdot h) * x = g * (h * x)$
- G is a commutative/abelian group
- For any $x, x' \in \mathcal{X}$, there exists a **unique** $g \in G$ such that $g * x = x'$

Group Actions – Basic Definitions

Definition

Group Action of a group $(G,\cdot)$ on a set $\mathcal{X}$ is a function $*: G \times \mathcal{X} \rightarrow \mathcal{X}$ such that:

- Letting e be the identity element in G, for every $x \in \mathcal{X}$ we have $e * x = x$
- For every $g, h \in G$ and for every $x \in \mathcal{X}$ we have $(g \cdot h) * x = g * (h * x)$
- G is a commutative/abelian group
- For any $x, x' \in \mathcal{X}$, there exists a **unique** $g \in G$ such that $g * x = x'$

Effective Group Action (EGA) : Can efficiently compute $g \star x$ for **any** $(g, x) \in G \times \mathcal{X}$

EGA Instantiations: CSIDH [CLMPR18] with known group structure, CSI-Fish [BKV19])

Not broken by the recent attacks on the SIDH family of isogenies!

Group Actions – Computational Assumptions

Definition

ow-EGA (one-way EGA, models DLog-CSIDH):

For $g \leftarrow G$ and $x \leftarrow \mathcal{X}$, given $(x, g * x)$, it is computationally infeasible to compute g

wU-EGA (weak Unpredictable-EGA, models computational-CSIDH):

For $g, h \leftarrow G$ and $x \leftarrow \mathcal{X}$, given $(x, g * x, h * x)$, it is computationally infeasible to compute $(g.h) * x$

Chapter IV

Round Optimal OT in Setup Model

Semi-honest Oblivious Transfer in Setup model

CRS: (x, x_0, x_1)

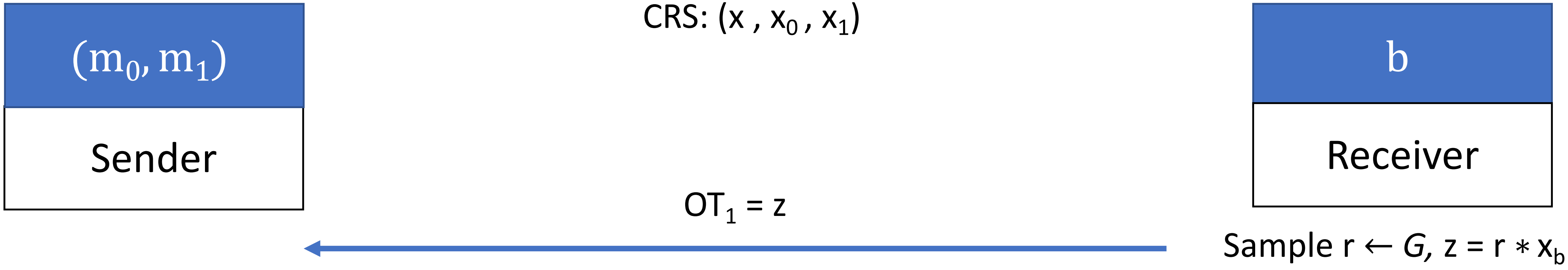
(m_0, m_1)

Sender

b

Receiver

Semi-honest Oblivious Transfer in Setup model



(m_0, m_1)

Sender

CRS: (x, x_0, x_1)

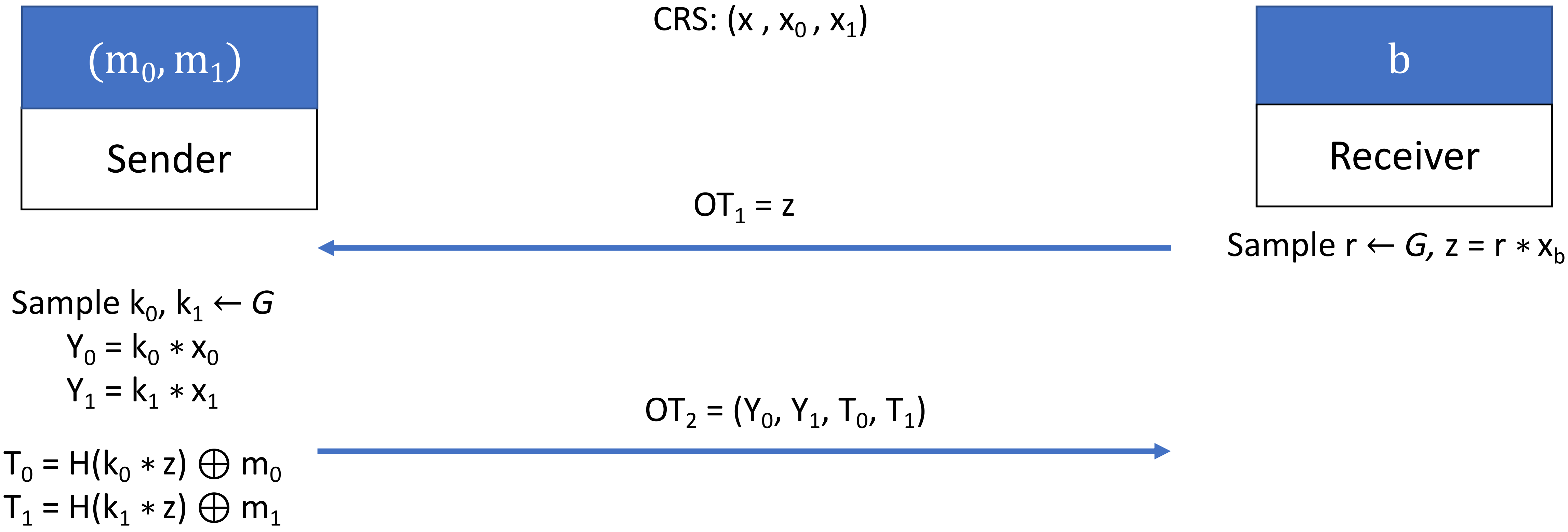
b

Receiver

$OT_1 = z$

Sample $r \leftarrow G$, $z = r * x_b$

Semi-honest Oblivious Transfer in Setup model



CRS: (x, x_0, x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z$

Sample $r \leftarrow G$, $z = r * x_b$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$

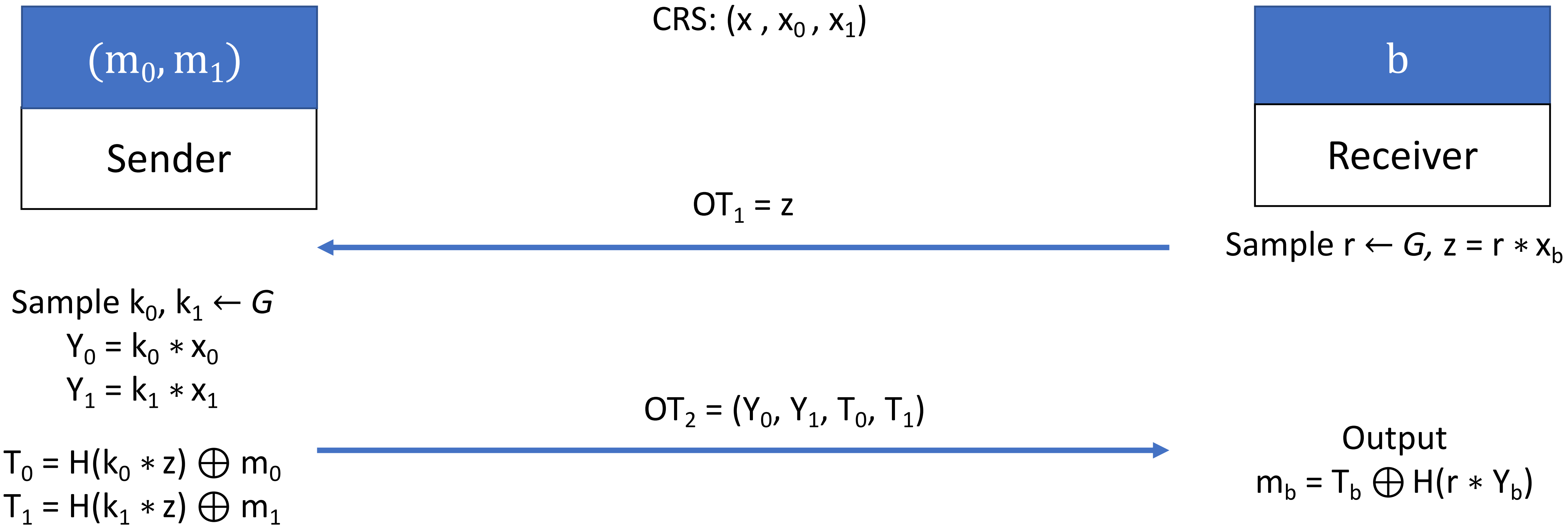
$Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$

$T_1 = H(k_1 * z) \oplus m_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

Semi-honest Oblivious Transfer in Setup model



CRS: (x, x_0, x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z$

Sample $r \leftarrow G$, $z = r * x_b$

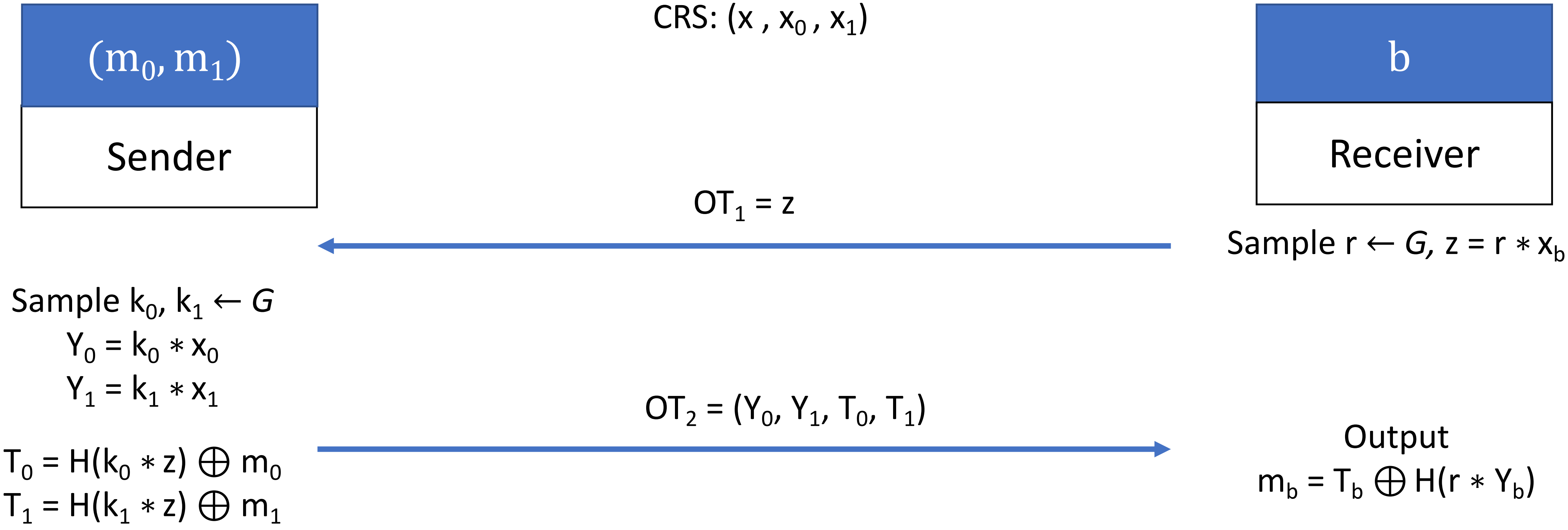
Sample $k_0, k_1 \leftarrow G$
$Y_0 = k_0 * x_0$
$Y_1 = k_1 * x_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

$T_0 = H(k_0 * z) \oplus m_0$
$T_1 = H(k_1 * z) \oplus m_1$

Output
$m_b = T_b \oplus H(r * Y_b)$

Semi-honest Oblivious Transfer in Setup model



CRS: (x, x_0, x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z$

Sample $r \leftarrow G$, $z = r \ast x_b$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 \ast x_0$

$Y_1 = k_1 \ast x_1$

$T_0 = H(k_0 \ast z) \oplus m_0$

$T_1 = H(k_1 \ast z) \oplus m_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

Output

$m_b = T_b \oplus H(r \ast Y_b)$

Receiver Privacy: Choice bit b is statistically hidden

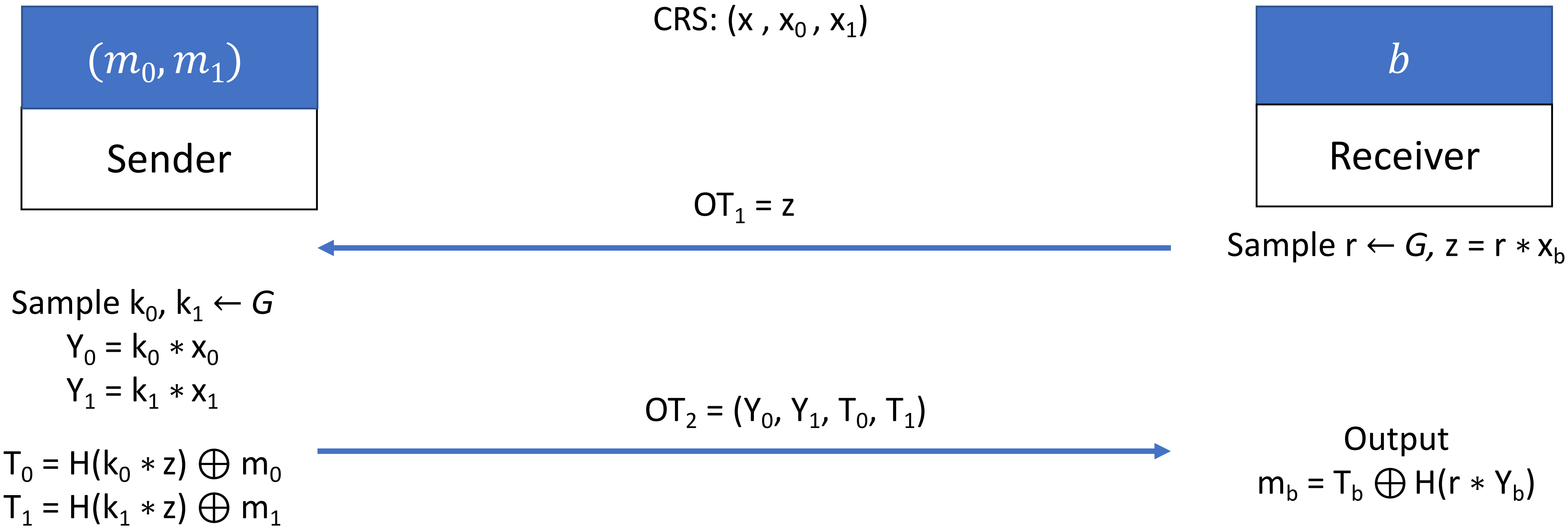
Assuming $b = 1$:

$z = r \ast x_1 = \mathbf{r'} \ast x_0$

where $\mathbf{r' = r\, g_1\, g_0^{-1}}$

for $x_0 = g_0 \ast x$, $x_1 = g_1 \ast x = g_1 \ast g_0^{-1} \ast x_0$

Semi-honest Oblivious Transfer in Setup model



CRS: (x, x_0, x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z$

Sample $r \leftarrow G$, $z = r * x_b$

Sample $k_0, k_1 \leftarrow G$
$Y_0 = k_0 * x_0$
$Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$
$T_1 = H(k_1 * z) \oplus m_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

Output
$m_b = T_b \oplus H(r * Y_b)$

Receiver Privacy: Choice bit b is statistically hidden

Sender Privacy: If Receiver computes m_{1-b} then break wu-EGA property
(Need to extract r for the reduction)

Semi-honest Oblivious Transfer in Setup model

CRS: (x, x_0, x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z$

Sample $r \leftarrow G$, $z = r * x_b$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$

$Y_1 = k_1 * x_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

$T_0 = H(k_0 * z) \oplus m_0$

$T_1 = H(k_1 * z) \oplus m_1$

Output

$m_b = T_b \oplus H(r * Y_b)$

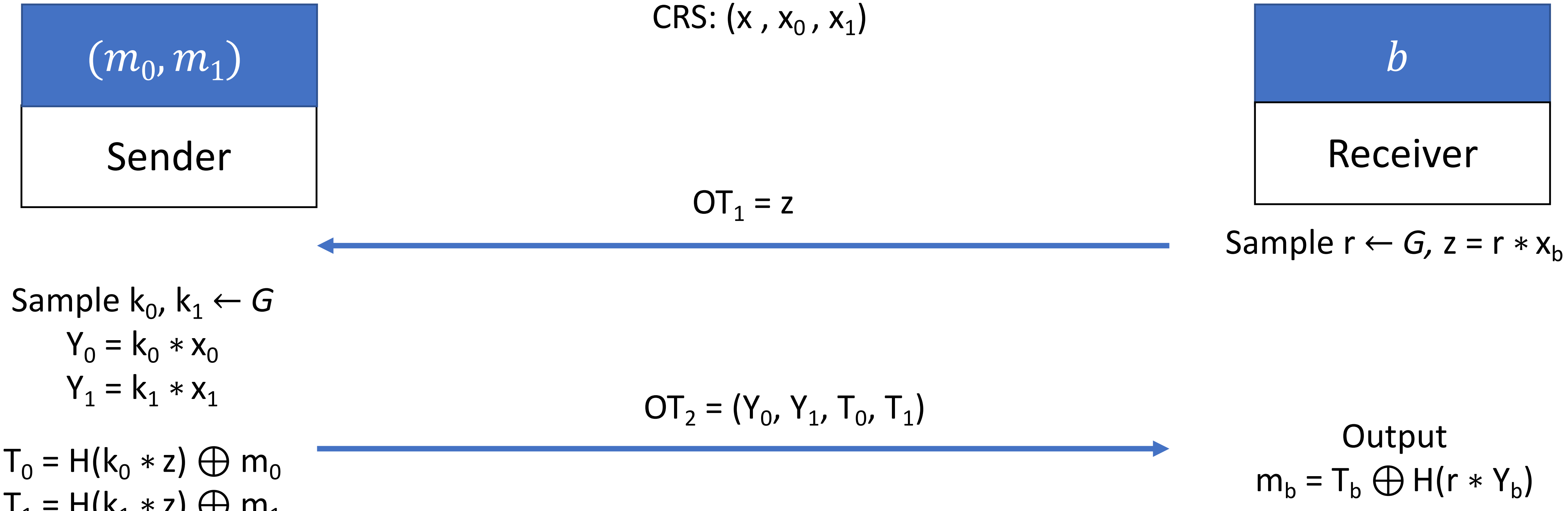
Secure against malicious sender

t b is statistically hidden

Sender Privacy: If Receiver computes m_{1-b} then break wu-EGA property

(Need to extract r for the reduction)

Semi-honest Oblivious Transfer in Setup model



CRS: (x , x_0 , x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z$

Sample $r \leftarrow G$, $z = r * x_b$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$

$Y_1 = k_1 * x_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

$T_0 = H(k_0 * z) \oplus m_0$

$T_1 = H(k_1 * z) \oplus m_1$

Output

$m_b = T_b \oplus H(r * Y_b)$

Secure against malicious sender

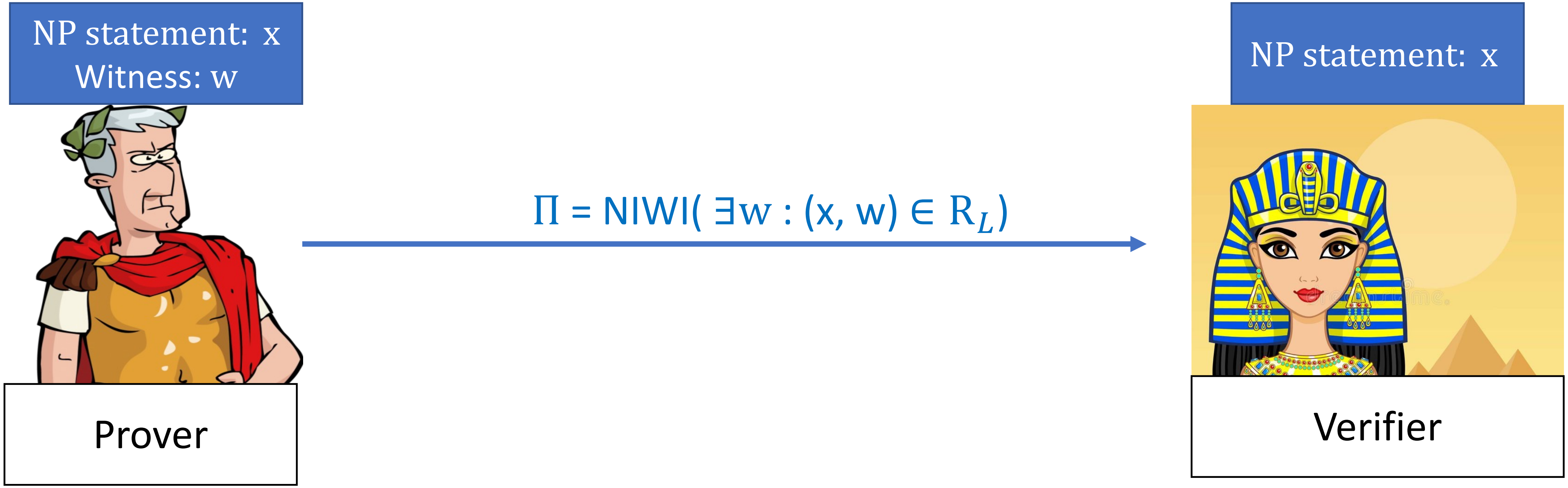
t b is statistically hidden

Need to extract b, r from Malicious receiver

Sender Privacy: If Receiver computes m_{1-b} then break wu-EGA property

(Need to extract r for the reduction)

Non-interactive Witness-Indistinguishability Proof-of-Knowledge (NIWI)



NP statement: x
Witness: w

Prover

Π = NIWI($\exists w : (x, w) \in R_L$)

NP statement: x

Verifier

Completeness: Verifier outputs 1 if $(x, w) \in R_L$

Soundness: If $x \notin L$, Verifier outputs 0 with high probability

Witness-Indistinguishability: $\Pi_0 \approx \Pi_1$ where Π_b is generated using witness w_b (where w_0 , w_1 are valid witness)

Proof-of-Knowledge: Witness w can be extracted from an accepting proof

Non-interactive Witness-Indistinguishability Proof-of-Knowledge (NIWI)

NP statement: x
Witness: w

Prover

Π = NIWI($\exists w : (x, w) \in R_L$)

NP statement: x

Verifier

Completeness: Verifier outputs 1 if $(x, w) \in R_L$

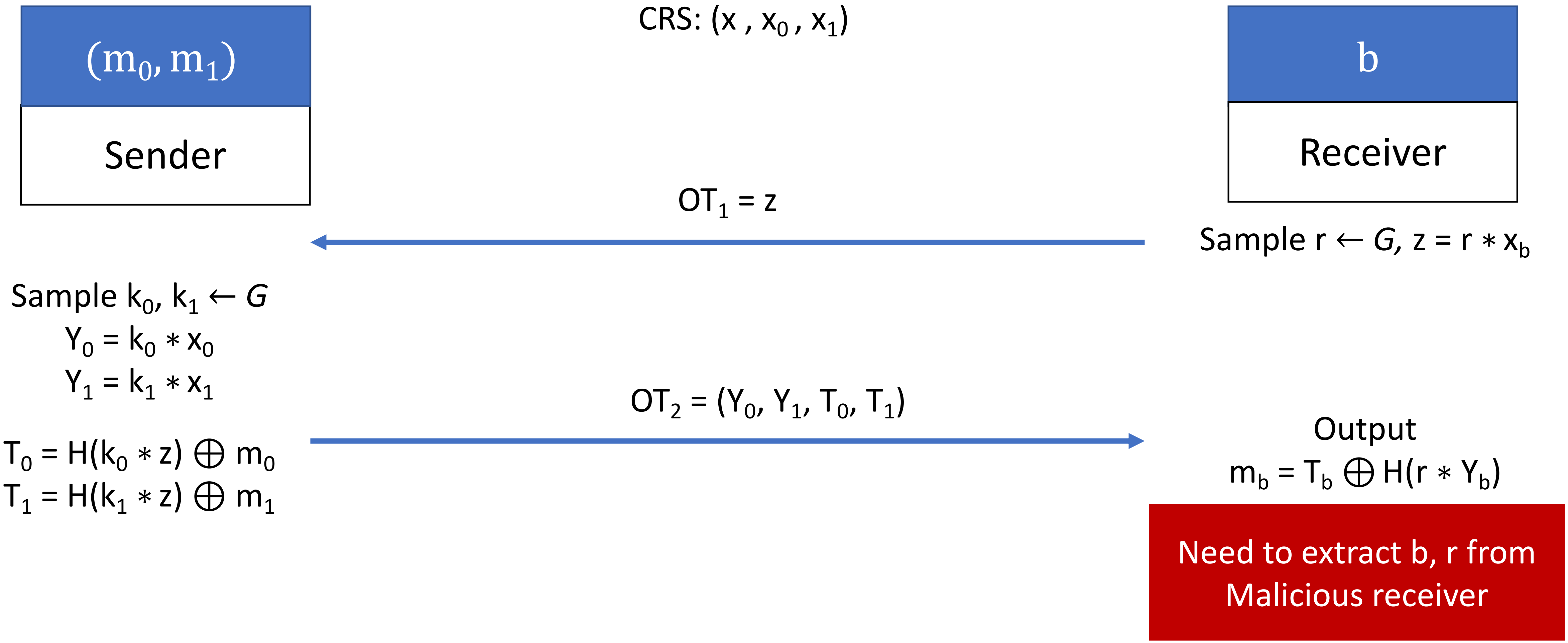
Soundness: If $x \notin L$, Verifier outputs 0 with high probability

Witness-Indistinguishability: $\Pi_0 \approx \Pi_1$ where Π_b is generated using witness w_b (where w_0 , w_1 are valid witness)

Proof-of-Knowledge: Witness w can be extracted from an accepting proof

Build from wu-EGA

Maliciously Secure Oblivious Transfer in Setup model



CRS: (x, x_0, x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z$

Sample $r \leftarrow G$, $z = r * x_b$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$

$Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$

$T_1 = H(k_1 * z) \oplus m_1$

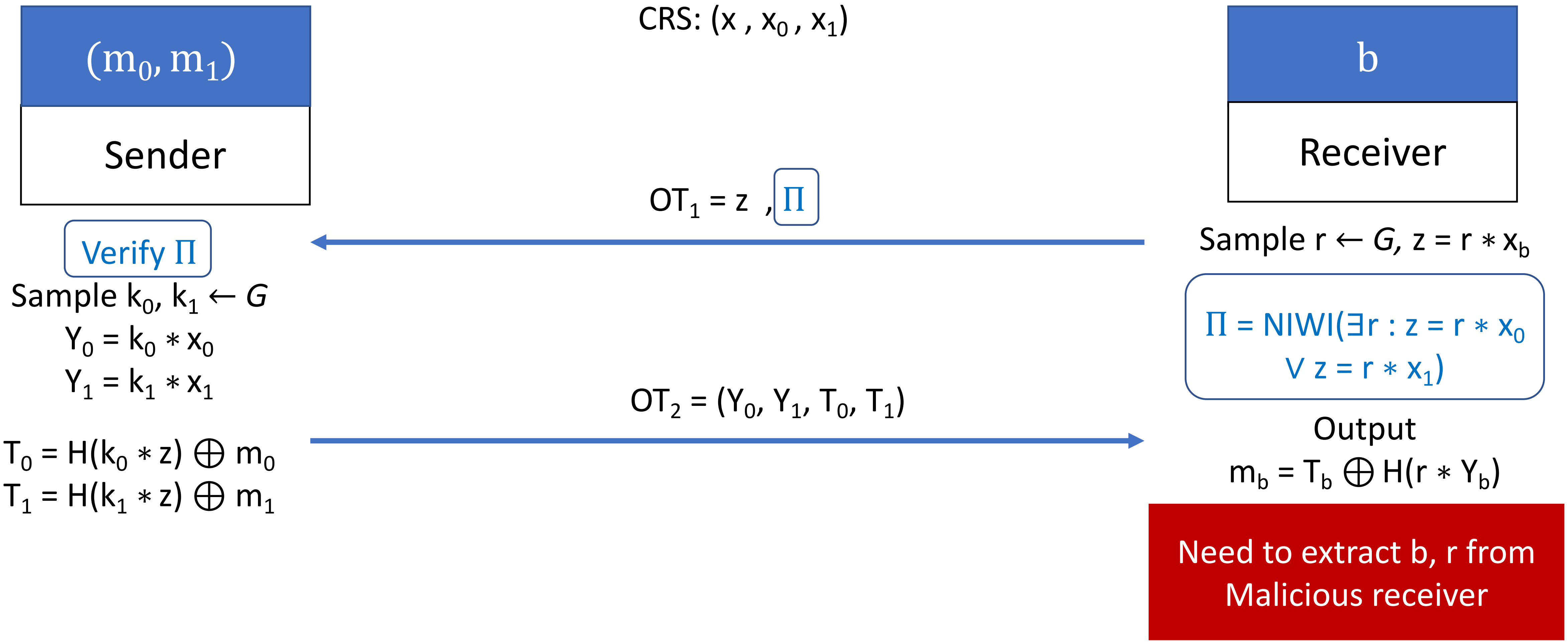
$OT_2 = (Y_0, Y_1, T_0, T_1)$

Output

$m_b = T_b \oplus H(r * Y_b)$

Need to extract b, r from Malicious receiver

Maliciously Secure Oblivious Transfer in Setup model



CRS: (x , x_0 , x_1)

(m_0, m_1)

Sender

b

Receiver

Sample $r \leftarrow G$, $z = r * x_b$

$\Pi = \mathrm{NIWI}(\exists r : z = r * x_0 \vee z = r * x_1)$

$OT_1 = z \ , \Pi$

Verify Π

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$

$Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$

$T_1 = H(k_1 * z) \oplus m_1$

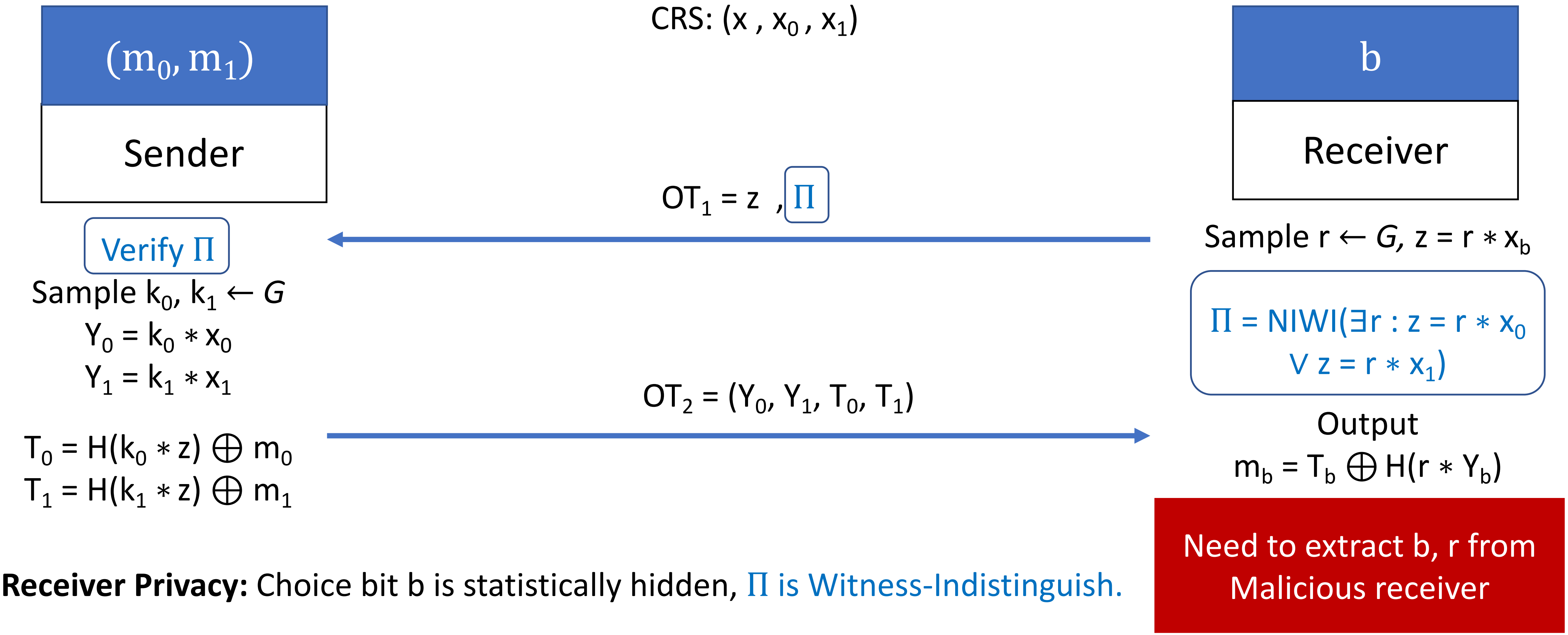
$OT_2 = (Y_0, Y_1, T_0, T_1)$

Output

$m_b = T_b \oplus H(r * Y_b)$

Need to extract b, r from Malicious receiver

Maliciously Secure Oblivious Transfer in Setup model **(Input Privacy)**



CRS: (x, x_0, x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z$, $\boxed{\Pi}$

Sample $r \leftarrow G$, $z = r * x_b$

Π = NIWI($\exists r : z = r * x_0 \vee z = r * x_1$)

Verify Π

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$

$Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$

$T_1 = H(k_1 * z) \oplus m_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

Output

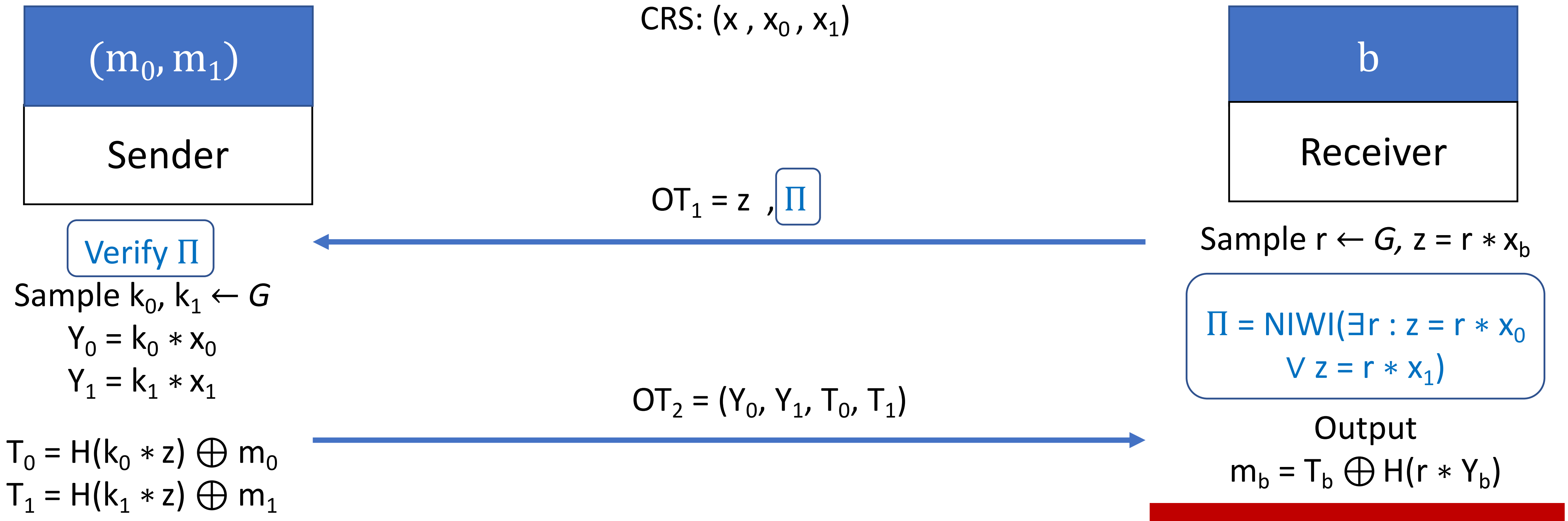
$m_b = T_b \oplus H(r * Y_b)$

Need to extract b, r from Malicious receiver

Receiver Privacy: Choice bit b is statistically hidden, Π is Witness-Indistinguish.

Sender Privacy: If Receiver computes $m_{1\text{-}b}$ then break wu-EGA property, Π is Sound and extractable
(Need to extract r for the reduction)

Maliciously Secure Oblivious Transfer in Setup model **(Input Extraction)**



CRS: (x, x_0, x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z\ ,\boxed{\Pi}$

Sample $r \leftarrow G$, $z = r * x_b$

$\Pi = \text{NIWI}(\exists r : z = r * x_0 \vee z = r * x_1)$

$\boxed{\text{Verify } \Pi}$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$

$Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$

$T_1 = H(k_1 * z) \oplus m_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

Output

$m_b = T_b \oplus H(r * Y_b)$

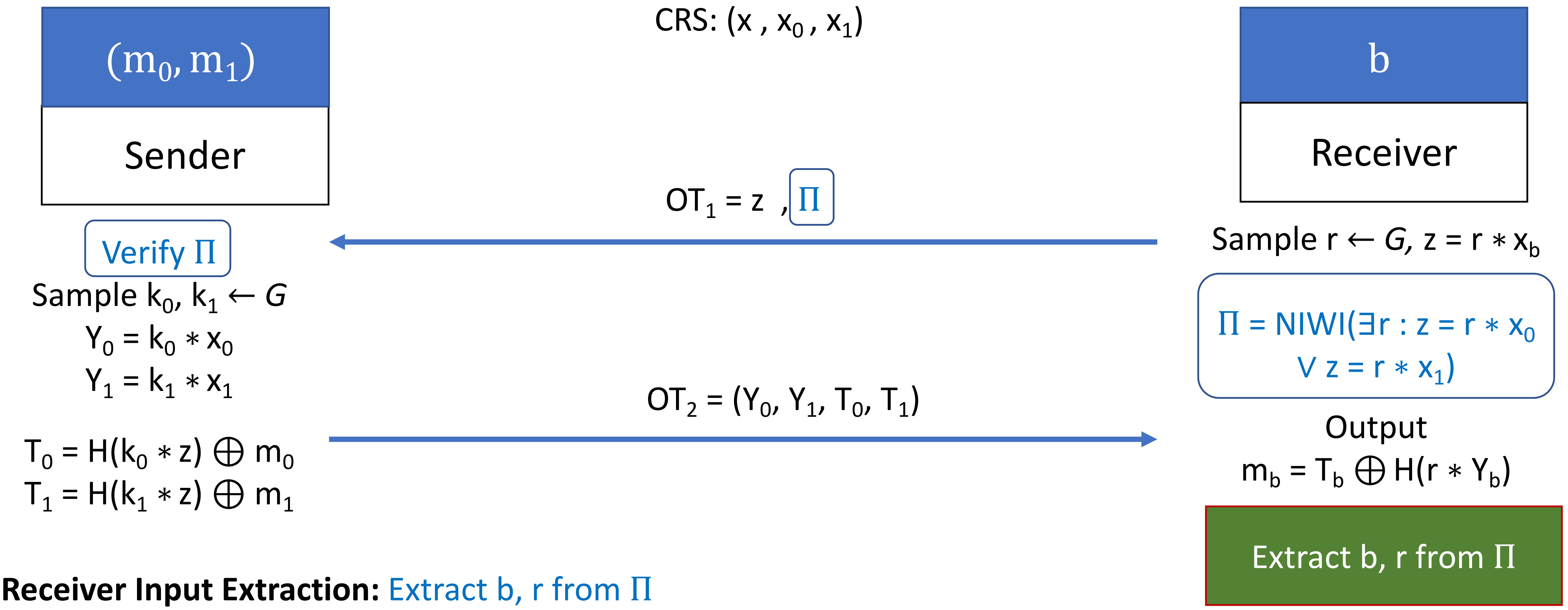
Need to extract b, r from Malicious receiver

Receiver Input Extraction: Extract b, r from Π

Sender Input Extraction: Compute m_1 by setting b = 1, extract m_0 by using the CRS trapdoor ($= g_1 * g_0^{-1}$)

Assuming b = 1: $z = r * x_1 = \mathbf{r'} * x_0$ (where $\mathbf{r' = r\, g_1\, g_0^{-1}}$ for $x_0 = g_0 * x$, $x_1 = g_1 * x = g_1 * g_0^{-1} * x_0$)

Maliciously Secure Oblivious Transfer in Setup model **(Input Extraction)**



CRS: (x , x_0 , x_1)

(m_0, m_1)

Sender

b

Receiver

$OT_1 = z\ , \boxed{\Pi}$

Sample $r \leftarrow G$, $z = r * x_b$

$\Pi = NIWI(\exists r : z = r * x_0 \lor z = r * x_1)$

$\boxed{\text{Verify } \Pi}$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$

$Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$

$T_1 = H(k_1 * z) \oplus m_1$

$OT_2 = (Y_0, Y_1, T_0, T_1)$

Output

$m_b = T_b \oplus H(r * Y_b)$

Extract b, r from Π

Receiver Input Extraction: Extract b, r from Π

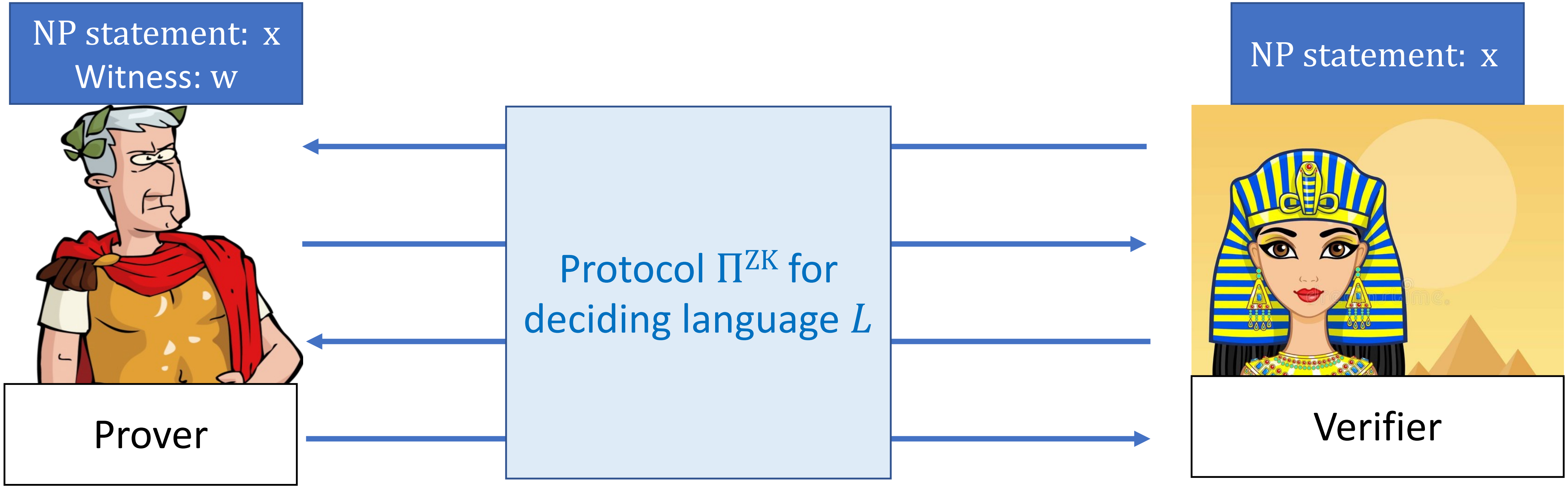
Sender Input Extraction: Compute m_1 by setting b = 1, extract m_0 by using the CRS trapdoor ($= g_1 * g_0^{-1}$)

Assuming b = 1: $z = r * x_1 = \mathbf{r'} * x_0$ (where $\mathbf{r' = r\, g_1\, g_0^{-1}}$ for $x_0 = g_0 * x$, $x_1 = g_1 * x = g_1 * g_0^{-1} * x_0$)

Chapter V

Round Optimal OT in Plain Model

Delayed-Input Zero-Knowledge Proof-of-Knowledge (ZK)



NP statement: x
Witness: w

Prover

Protocol Π^{ZK} for deciding language L

NP statement: x

Verifier

Completeness: Verifier outputs 1 if $(\mathrm{x}, \mathrm{w}) \in \mathrm{R}_L$

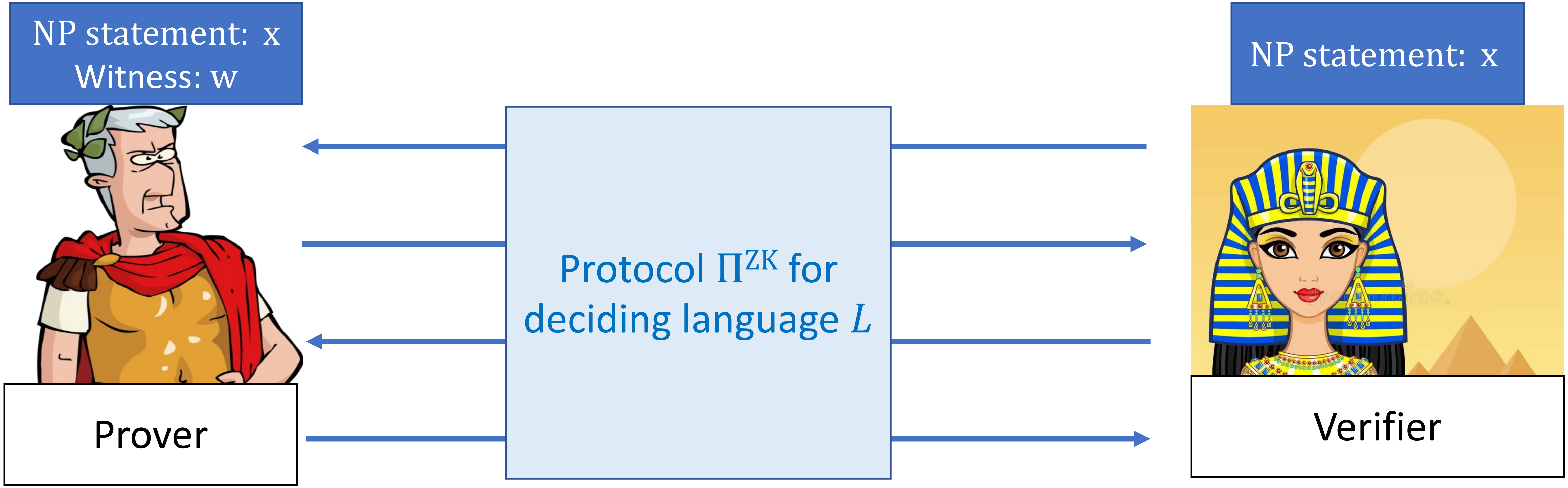
Soundness: If $\mathrm{x} \notin L$, Verifier outputs 0 with high probability

Zero-Knowledge: Π leaks no information about w to the Verifier

Proof-of-Knowledge: Witness w can be extracted from an accepting proof

Delayed-Input: Only the last ZK protocol message depends on statement x

Delayed-Input Zero-Knowledge Proof-of-Knowledge (ZK)



NP statement: x
Witness: w

Prover

Protocol Π^{ZK} for deciding language L

NP statement: x

Verifier

Completeness: Verifier outputs 1 if $(\mathrm{x}, \mathrm{w}) \in \mathrm{R}_L$

Soundness: If $\mathrm{x} \notin L$, Verifier outputs 0 with high probability

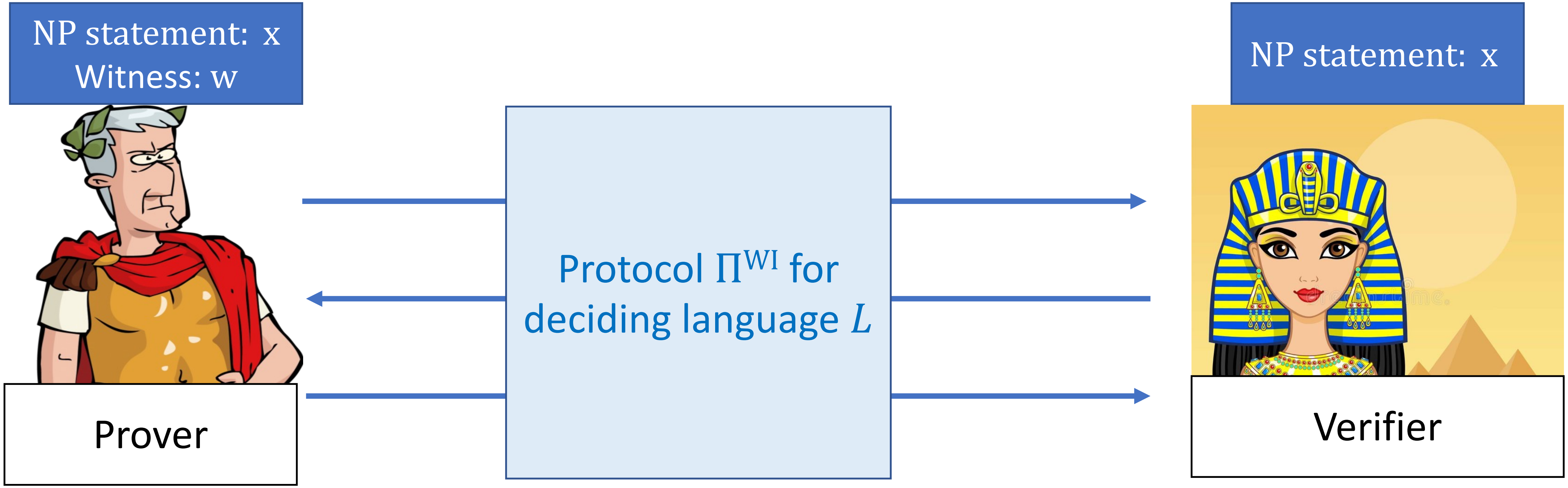
Zero-Knowledge: Π leaks no information about w to the Verifier

Proof-of-Knowledge: Witness w can be extracted from an accepting proof

Delayed-Input: Only the last ZK protocol message depends on statement x

Build from wu-EGA

Delayed-Input Witness-Indistinguishability Proof-of-Knowledge (WI)



NP statement: x
Witness: w

Prover

Protocol Π^{WI} for deciding language L

NP statement: x

Verifier

Completeness: Verifier outputs 1 if $(\mathrm{x}, \mathrm{w}) \in \mathrm{R}_L$

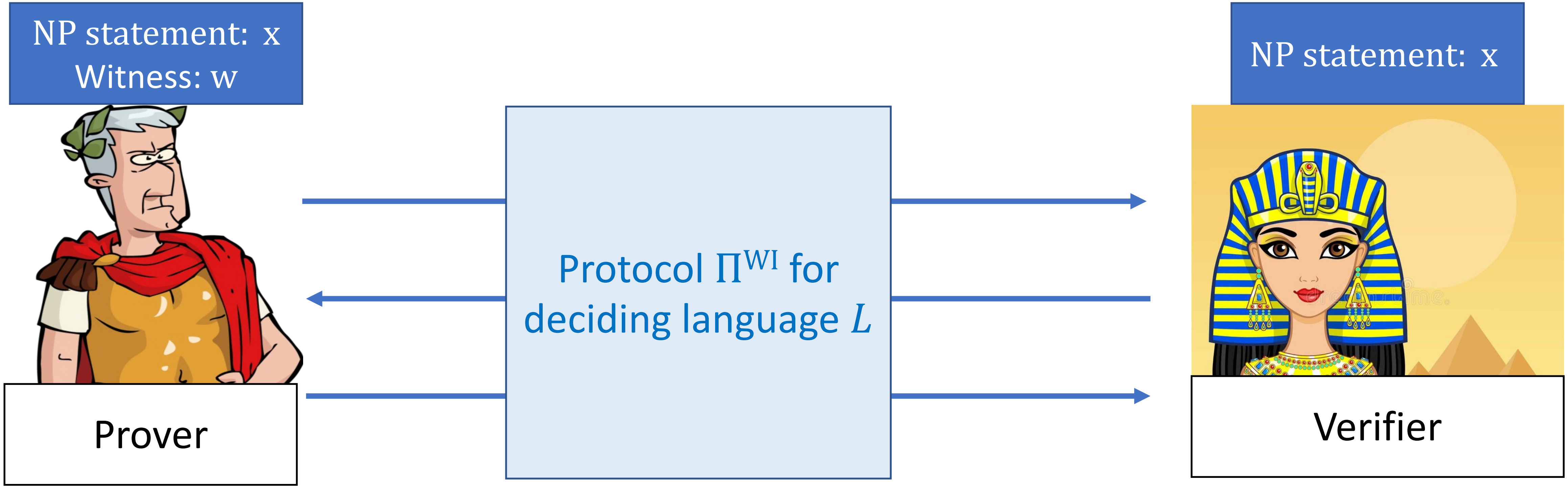
Soundness: If $\mathrm{x} \notin L$, Verifier outputs 0 with high probability

Witness-Indistinguishability: $\Pi_0 \approx \Pi_1$ where Π_b is generated using witness w_b (where w_0 , w_1 are valid witness)

Proof-of-Knowledge: Witness w can be extracted from an accepting proof

Delayed-Input: Only the last WI protocol message depends on statement x

Delayed-Input Witness-Indistinguishability Proof-of-Knowledge (WI)



NP statement: x
Witness: w

Prover

Protocol Π^{WI} for deciding language L

NP statement: x

Verifier

Completeness: Verifier outputs 1 if $(\mathrm{x}, \mathrm{w}) \in \mathrm{R}_L$

Soundness: If $\mathrm{x} \notin L$, Verifier outputs 0 with high probability

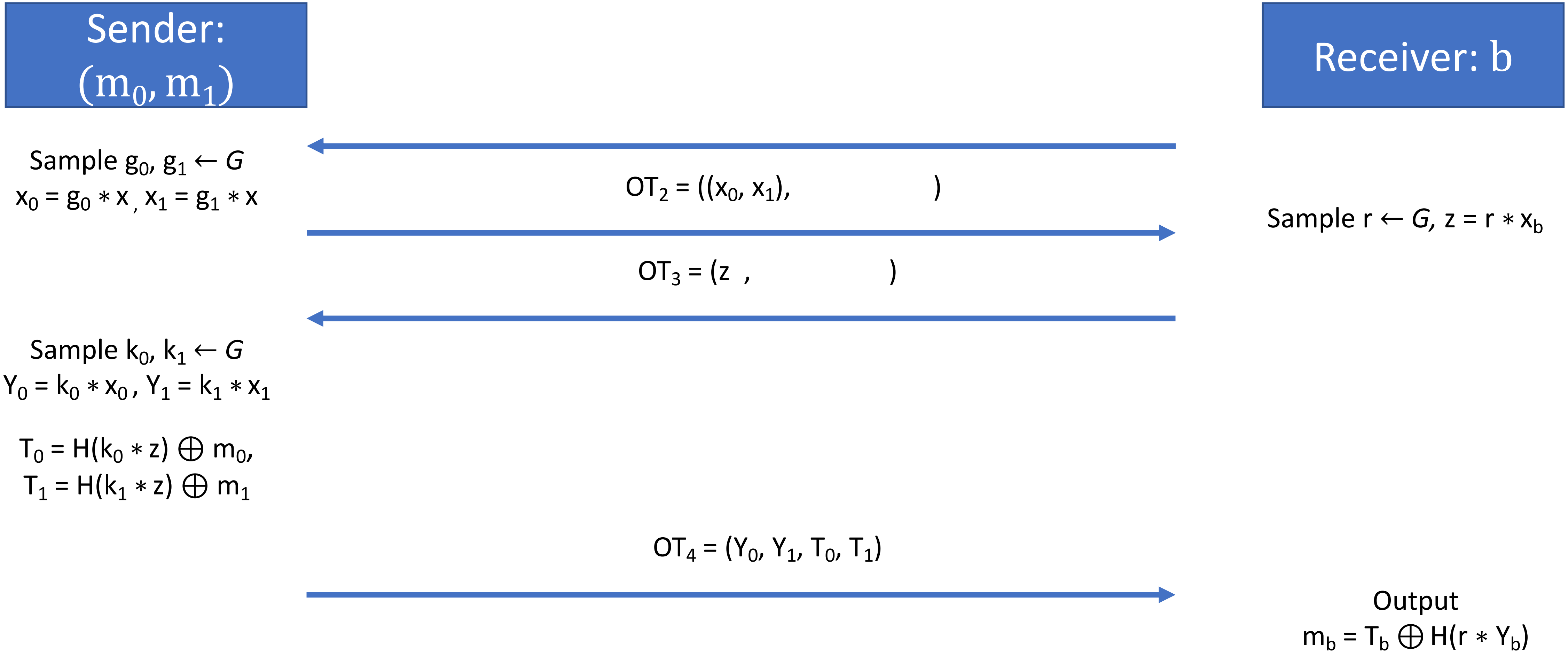
Witness-Indistinguishability: $\Pi_0 \approx \Pi_1$ where Π_b is generated using witness w_b (where w_0 , w_1 are valid witness)

Proof-of-Knowledge: Witness w can be extracted from an accepting proof

Delayed-Input: Only the last WI protocol message depends on statement x

Build from wu-EGA

Maliciously Secure Oblivious Transfer in Plain model



Sender: (m_0, m_1)

Receiver: b

Sample $g_0, g_1 \leftarrow G$
$x_0 = g_0 * x$, $x_1 = g_1 * x$

$OT_2 = ((x_0, x_1),\qquad\qquad)$

Sample $r \leftarrow G$, $z = r * x_b$

$OT_3 = (z\ ,\qquad\qquad)$

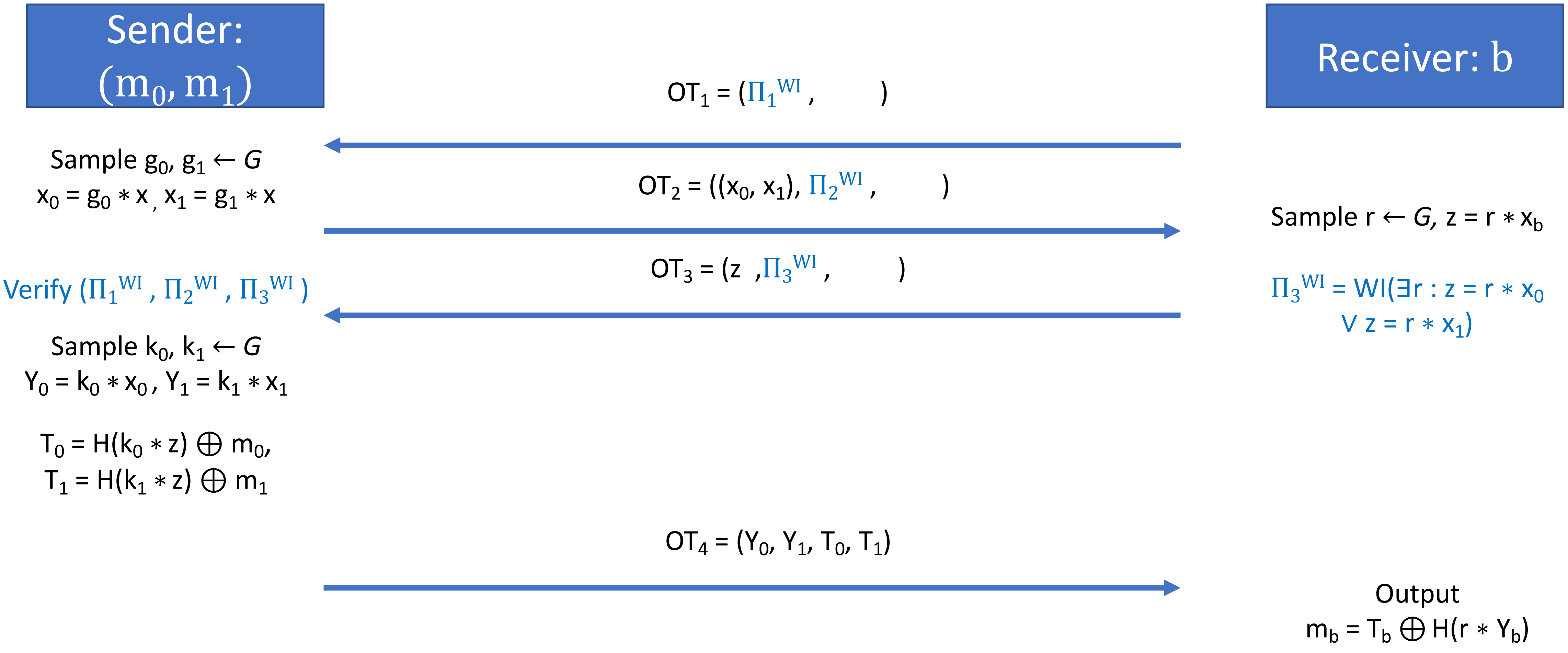
Sample $k_0, k_1 \leftarrow G$
$Y_0 = k_0 * x_0$, $Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$,
$T_1 = H(k_1 * z) \oplus m_1$

$OT_4 = (Y_0, Y_1, T_0, T_1)$

Output
$m_b = T_b \oplus H(r * Y_b)$

Maliciously Secure Oblivious Transfer in Plain model **(Input Privacy)**



Sender: (m_0, m_1)

Receiver: b

$OT_1 = (\Pi_1^{WI} , \quad)$

Sample $g_0, g_1 \leftarrow G$

$x_0 = g_0 * x$, $x_1 = g_1 * x$

$OT_2 = ((x_0, x_1), \Pi_2^{WI} , \quad)$

Sample $r \leftarrow G$, $z = r * x_b$

$OT_3 = (z \ ,\Pi_3^{WI} , \quad)$

$\Pi_3^{WI} = WI(\exists r : z = r * x_0 \vee z = r * x_1)$

Verify $(\Pi_1^{WI} , \Pi_2^{WI} , \Pi_3^{WI})$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0 , Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0,$

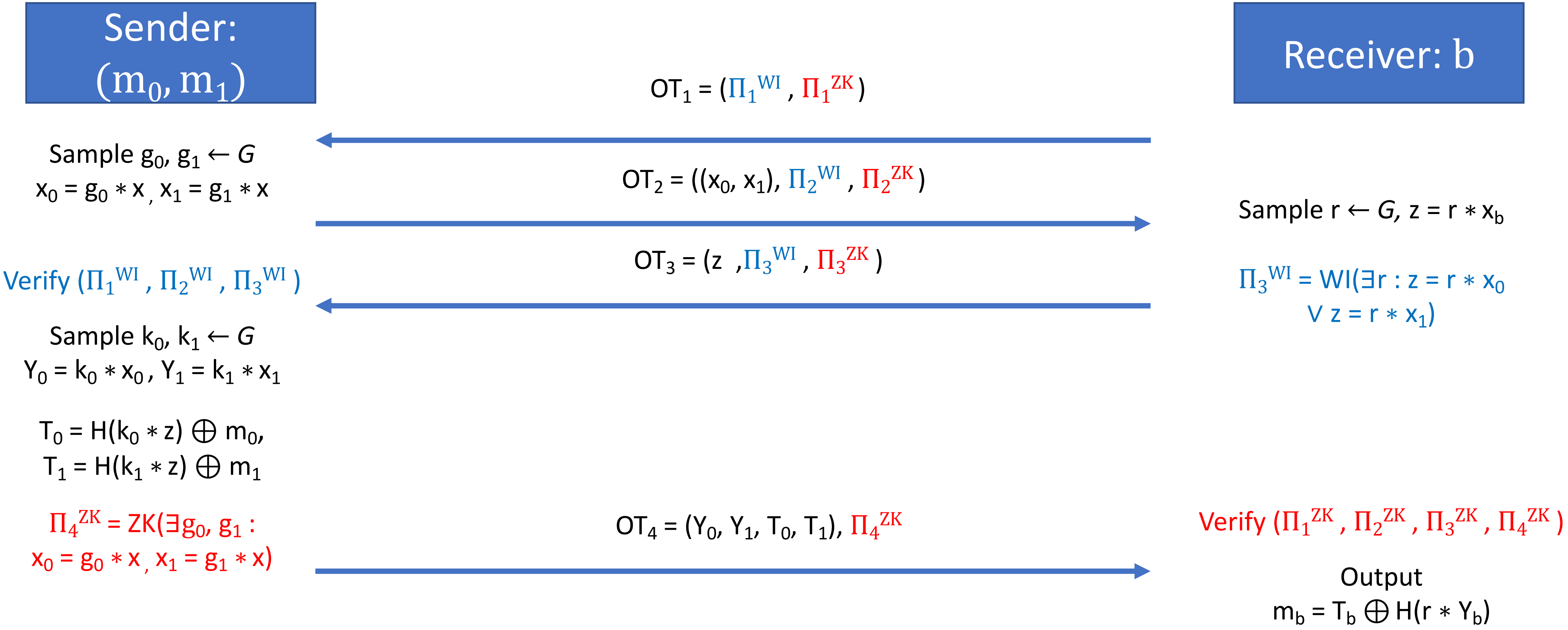
$T_1 = H(k_1 * z) \oplus m_1$

$OT_4 = (Y_0, Y_1, T_0, T_1)$

Output

$m_b = T_b \oplus H(r * Y_b)$

Maliciously Secure Oblivious Transfer in Plain model **(Input Privacy)**



Sender:
(m_0, m_1)

Receiver: b

$OT_1 = (\Pi_1^{WI}, \Pi_1^{ZK})$

Sample $g_0, g_1 \leftarrow G$
$x_0 = g_0 * x , x_1 = g_1 * x$

$OT_2 = ((x_0, x_1), \Pi_2^{WI}, \Pi_2^{ZK})$

Sample $r \leftarrow G, z = r * x_b$

$\Pi_3^{WI} = WI(\exists r : z = r * x_0$
$\vee z = r * x_1)$

$OT_3 = (z ,\Pi_3^{WI}, \Pi_3^{ZK})$

Verify $(\Pi_1^{WI}, \Pi_2^{WI}, \Pi_3^{WI})$

Sample $k_0, k_1 \leftarrow G$
$Y_0 = k_0 * x_0 , Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0,$
$T_1 = H(k_1 * z) \oplus m_1$

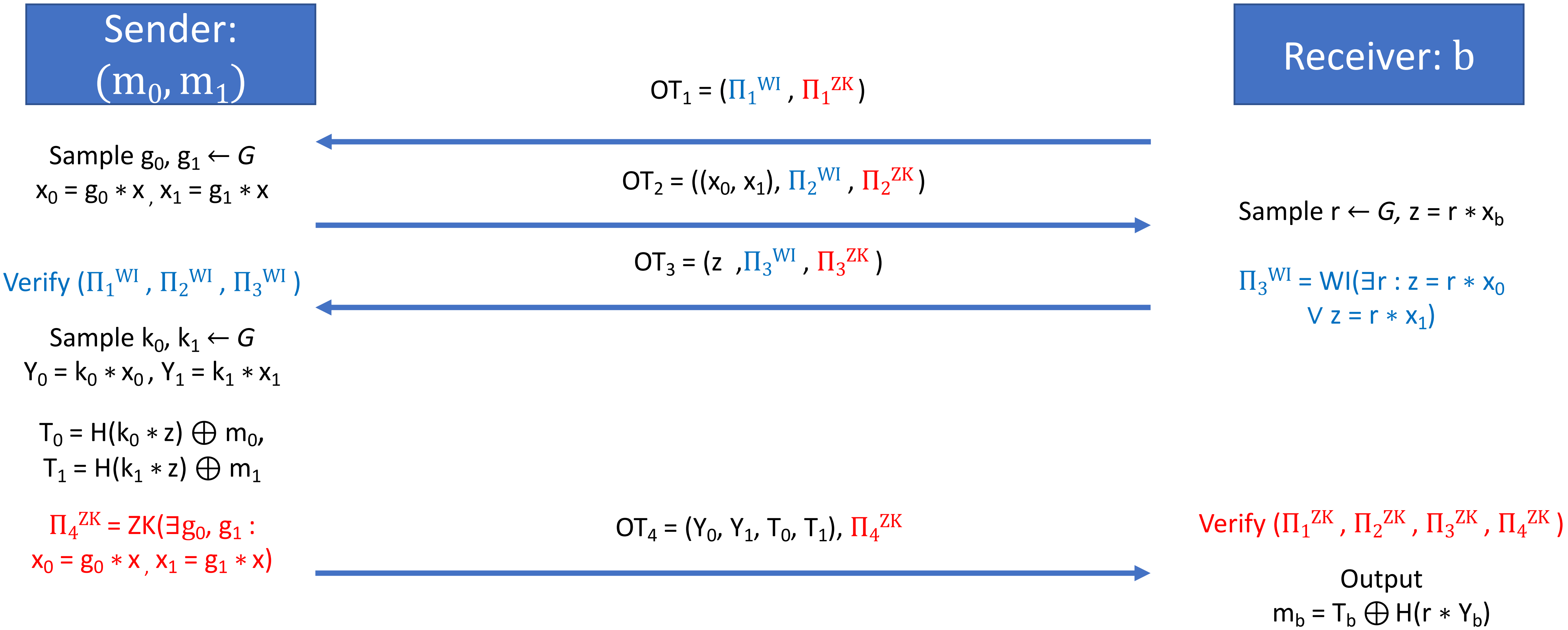
$\Pi_4^{ZK} = ZK(\exists g_0, g_1 :$
$x_0 = g_0 * x , x_1 = g_1 * x)$

$OT_4 = (Y_0, Y_1, T_0, T_1), \Pi_4^{ZK}$

Verify $(\Pi_1^{ZK}, \Pi_2^{ZK}, \Pi_3^{ZK}, \Pi_4^{ZK})$

Output
$m_b = T_b \oplus H(r * Y_b)$

Maliciously Secure Oblivious Transfer in Plain model **(Input Privacy)**



Sender: (m_0, m_1)

Receiver: b

$OT_1 = (\Pi_1^{WI}, \Pi_1^{ZK})$

Sample $g_0, g_1 \leftarrow G$
$x_0 = g_0 * x, x_1 = g_1 * x$

$OT_2 = ((x_0, x_1), \Pi_2^{WI}, \Pi_2^{ZK})$

Sample $r \leftarrow G$, $z = r * x_b$

$OT_3 = (z, \Pi_3^{WI}, \Pi_3^{ZK})$

$\Pi_3^{WI} = WI(\exists r : z = r * x_0 \lor z = r * x_1)$

Verify $(\Pi_1^{WI}, \Pi_2^{WI}, \Pi_3^{WI})$

Sample $k_0, k_1 \leftarrow G$
$Y_0 = k_0 * x_0, Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0,$
$T_1 = H(k_1 * z) \oplus m_1$

$\Pi_4^{ZK} = ZK(\exists g_0, g_1 :$
$x_0 = g_0 * x, x_1 = g_1 * x)$

$OT_4 = (Y_0, Y_1, T_0, T_1), \Pi_4^{ZK}$

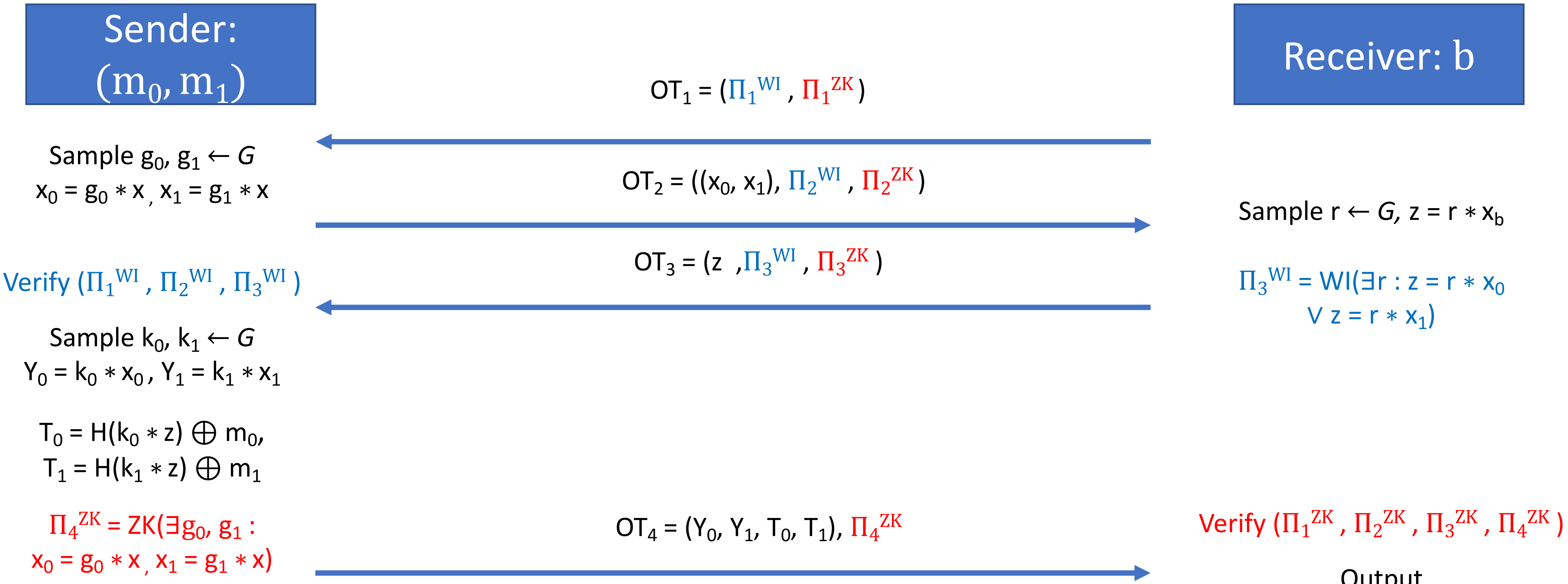
Verify $(\Pi_1^{ZK}, \Pi_2^{ZK}, \Pi_3^{ZK}, \Pi_4^{ZK})$

Output
$m_b = T_b \oplus H(r * Y_b)$

Receiver Privacy: b is statistically hidden, Π^{WI} is Witness-Indistinguishable, Π^{ZK} is Sound

Sender Privacy: If R computes m_{1-b} then break wu-EGA property, Π^{WI} is Sound, Π^{ZK} is Zero Knowledge

Maliciously Secure Oblivious Transfer in Plain model **(Input Extraction)**



Sender: (m_0, m_1)

Receiver: b

$OT_1 = (\Pi_1^{WI}, \Pi_1^{ZK})$

Sample $g_0, g_1 \leftarrow G$
$x_0 = g_0 * x, x_1 = g_1 * x$

$OT_2 = ((x_0, x_1), \Pi_2^{WI}, \Pi_2^{ZK})$

Sample $r \leftarrow G$, $z = r * x_b$

$OT_3 = (z, \Pi_3^{WI}, \Pi_3^{ZK})$

$\Pi_3^{WI} = WI(\exists r : z = r * x_0 \lor z = r * x_1)$

Verify $(\Pi_1^{WI}, \Pi_2^{WI}, \Pi_3^{WI})$

Sample $k_0, k_1 \leftarrow G$
$Y_0 = k_0 * x_0, Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0,$
$T_1 = H(k_1 * z) \oplus m_1$

$\Pi_4^{ZK} = ZK(\exists g_0, g_1 : x_0 = g_0 * x, x_1 = g_1 * x)$

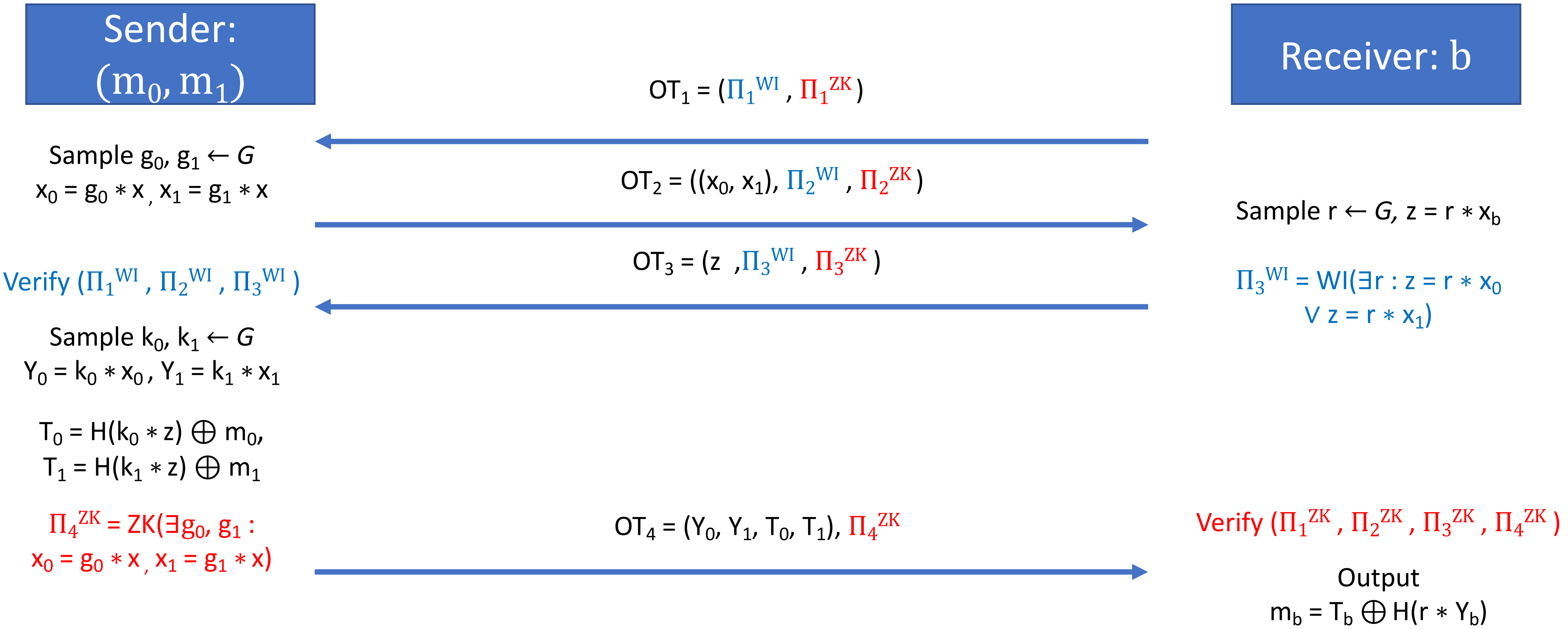
$OT_4 = (Y_0, Y_1, T_0, T_1), \Pi_4^{ZK}$

Verify $(\Pi_1^{ZK}, \Pi_2^{ZK}, \Pi_3^{ZK}, \Pi_4^{ZK})$

Output
$m_b = T_b \oplus H(r * Y_b)$

Receiver Input Extraction: Extract r from Π^{WI}, set b where $z = r * x_b$

Maliciously Secure Oblivious Transfer in Plain model **(Input Extraction)**



Sender: (m_0, m_1)

Receiver: b

$OT_1 = (\Pi_1^{WI}, \Pi_1^{ZK})$

Sample $g_0, g_1 \leftarrow G$

$x_0 = g_0 * x$, $x_1 = g_1 * x$

$OT_2 = ((x_0, x_1), \Pi_2^{WI}, \Pi_2^{ZK})$

Sample $r \leftarrow G$, $z = r * x_b$

$OT_3 = (z, \Pi_3^{WI}, \Pi_3^{ZK})$

Verify $(\Pi_1^{WI}, \Pi_2^{WI}, \Pi_3^{WI})$

$\Pi_3^{WI} = WI(\exists r : z = r * x_0 \lor z = r * x_1)$

Sample $k_0, k_1 \leftarrow G$

$Y_0 = k_0 * x_0$, $Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0$,

$T_1 = H(k_1 * z) \oplus m_1$

$\Pi_4^{ZK} = ZK(\exists g_0, g_1 : x_0 = g_0 * x, x_1 = g_1 * x)$

$OT_4 = (Y_0, Y_1, T_0, T_1), \Pi_4^{ZK}$

Verify $(\Pi_1^{ZK}, \Pi_2^{ZK}, \Pi_3^{ZK}, \Pi_4^{ZK})$

Output

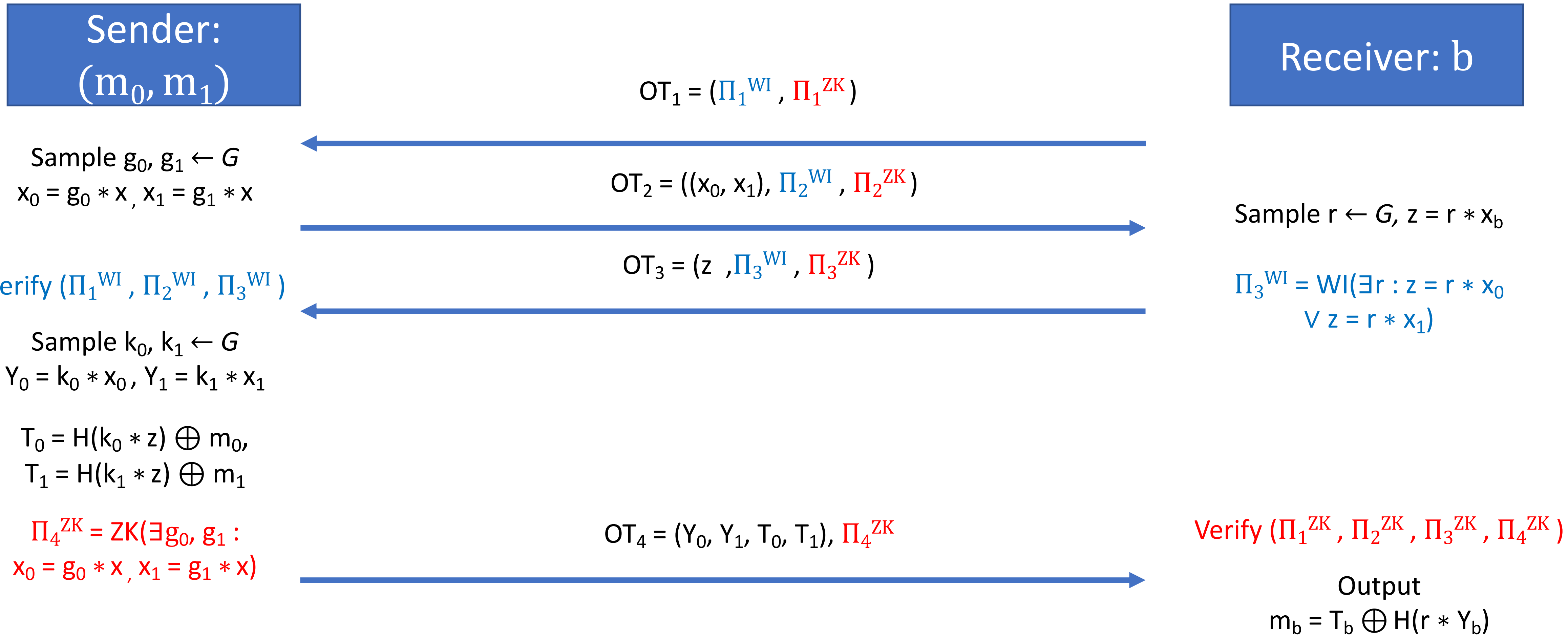
$m_b = T_b \oplus H(r * Y_b)$

Receiver Input Extraction: Extract r from Π^{WI}, set b where $z = r * x_b$

Sender Input Extraction: Extract (g_0, g_1) from Π^{ZK},

Compute m_1 by setting b = 1, Extract m_0 using $g_1 * g_0^{-1}$

Maliciously Secure Oblivious Transfer in Plain model **(Input Extraction)**



Sender: (m_0, m_1)

Receiver: b

$OT_1 = (\Pi_1^{WI}, \Pi_1^{ZK})$

Sample $g_0, g_1 \leftarrow G$
$x_0 = g_0 * x, x_1 = g_1 * x$

$OT_2 = ((x_0, x_1), \Pi_2^{WI}, \Pi_2^{ZK})$

Sample $r \leftarrow G$, $z = r * x_b$

$\Pi_3^{WI} = WI(\exists r : z = r * x_0$
$\vee z = r * x_1)$

$OT_3 = (z, \Pi_3^{WI}, \Pi_3^{ZK})$

Verify $(\Pi_1^{WI}, \Pi_2^{WI}, \Pi_3^{WI})$

Sample $k_0, k_1 \leftarrow G$
$Y_0 = k_0 * x_0, Y_1 = k_1 * x_1$

$T_0 = H(k_0 * z) \oplus m_0,$
$T_1 = H(k_1 * z) \oplus m_1$

$\Pi_4^{ZK} = ZK(\exists g_0, g_1 :$
$x_0 = g_0 * x, x_1 = g_1 * x)$

$OT_4 = (Y_0, Y_1, T_0, T_1), \Pi_4^{ZK}$

Verify $(\Pi_1^{ZK}, \Pi_2^{ZK}, \Pi_3^{ZK}, \Pi_4^{ZK})$

Output
$m_b = T_b \oplus H(r * Y_b)$

Receiver Input Extraction: Extract r from Π^{WI}, set b where $z = r * x_b$

Sender Input Extraction: Extract (g_0, g_1) from Π^{ZK},
Compute m_1 by setting b = 1, Extract m_0 using $g_1 * g_0^{-1}$

Build Π^{ZK}, Π^{WI} from wu-EGA

Chapter VI

Concluding Remarks

Conclusion

- Round Optimal OT/MPC Results in CRS+Random Oracle Model from computational-CSIDH
- Round Optimal OT/MPC Results in Plain Model from computational-CSIDH
- Oblivious Transfer Extension based on Reciprocal-CSIDH

Open Problems:

  - 2-round computational-CSIDH based UC-OT without Random Oracle?
  - Efficient (incurring O(1) isogeny computations) 2-round UC-OT from computational-CSIDH ?

Thank You

eprint.iacr.org/
2022/1511