Oblivious Transfer (OT) and OT Extension

School on Secure Multiparty Computation

Arpita Patra

INDIAN INSTITUTE OF SCIENCE
भारतीय विज्ञान संस्थान

Computer Science and Automation

Roadmap

- Oblivious Transfer

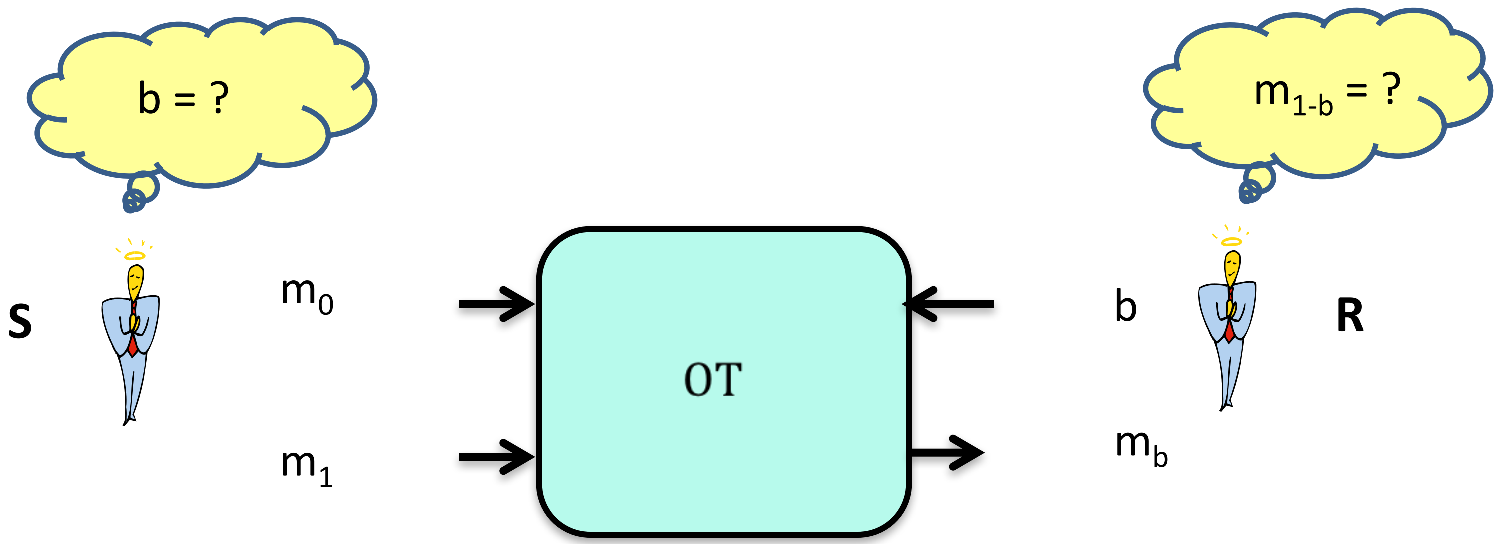
  - Construction from `special' PKE

- OT Extension

  - IKNP OT extension

- Tracing the journey of OT extension and some open questions

Oblivious Transfer



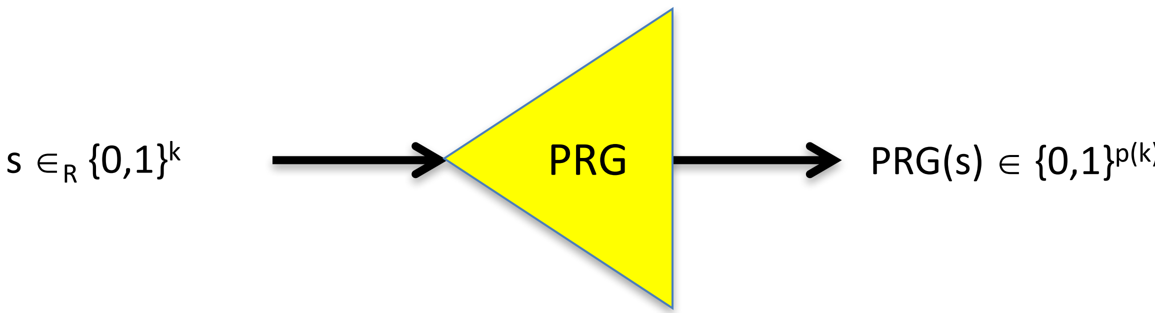
- **Complete** for MPC
- Used in both traditional approaches: Yao (per input) and GMW (per AND gate)
- OT forms the basis for most of the practical MPCs/2PCs, special purpose problems PSI
- OTs are **intrinsically expensive**- usually based on public key primitives
- AES Circuit: Millions of AND gates

Setting the stage for OT Extension

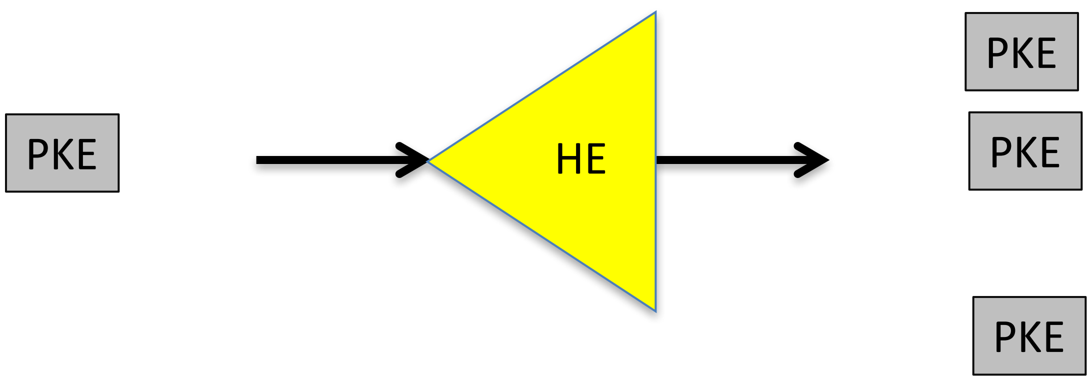
- X (task/object): executing/generating X is not very efficient

- Small no. X → many no. X

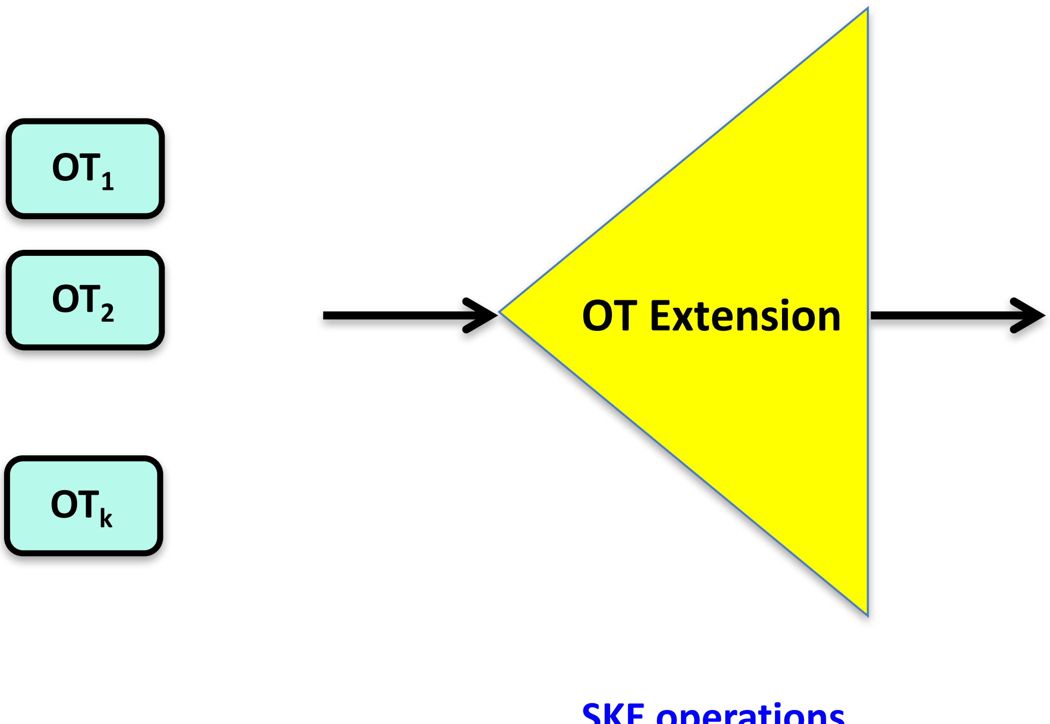
  - **PRG:** Truly Random short Seed → huge (pseudo-)random string



  - **Hybrid Encryption (HE):** one instance of PKE → many instances of PKE @ SKE operations



OT Extension: From small to many



SKE operations

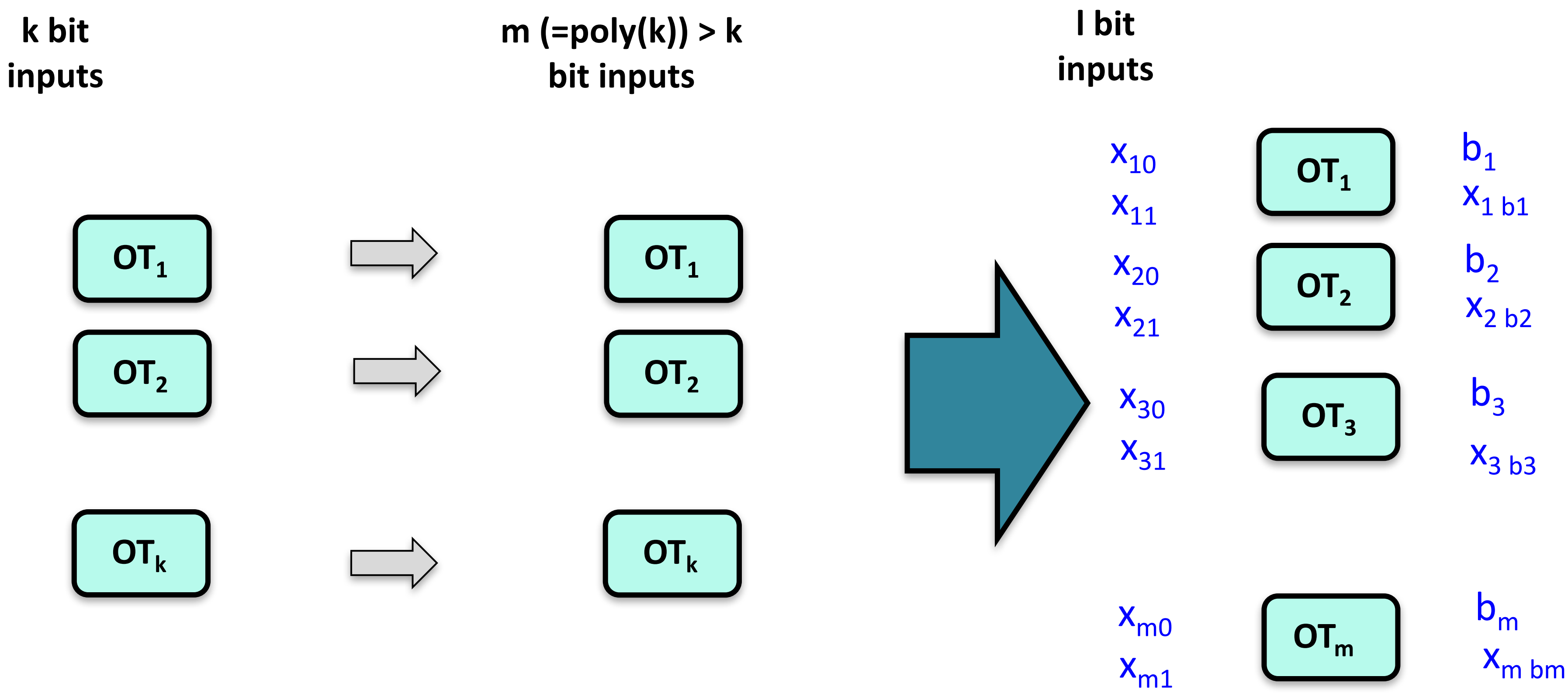
> OT Ext is not possible information theoretically [Bea96]

First work to tell us about OTExt

> OT Ext implies OWF [LZ13]

k: security parameter

Roadmap for Building OT Extension [IKNP03]

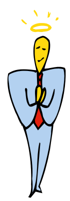


k OTs with k bit inputs —Domain Extension→ **k OTs with m > k bit inputs** —OT Extension→ **m OTs with m > k bit inputs**

Transformation I: Domain Extension

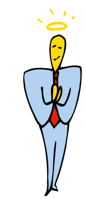
PRG $G: \{0,1\}^k \rightarrow \{0,1\}^{m=p(k)}$

k bit inputs

P_0 

$k_0 \rightarrow$ **OT** $\leftarrow b$

$k_1 \rightarrow$ **OT** $\rightarrow k_b$

 **P_1**

m_0

m_1

m bit inputs

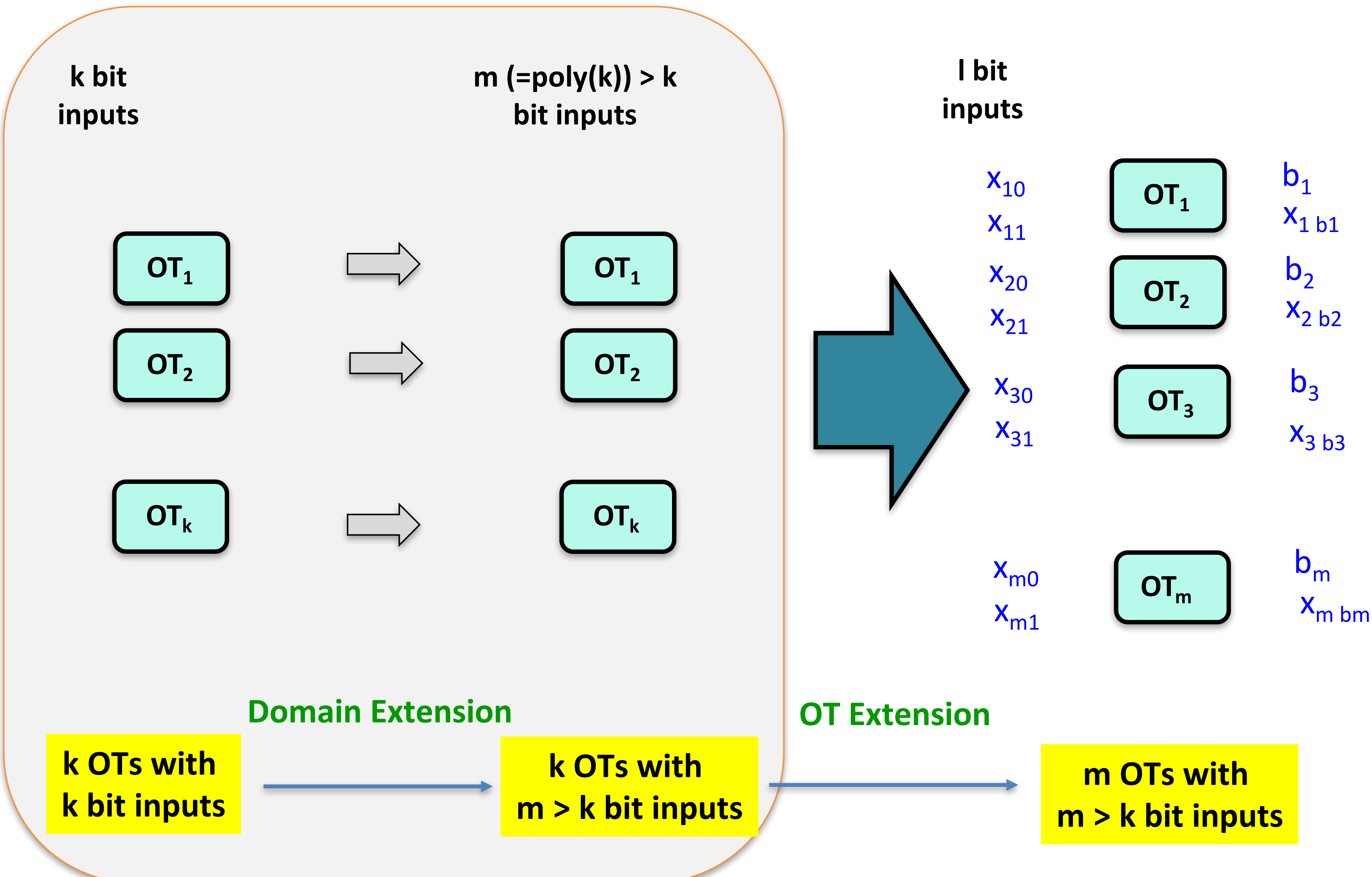
$y_0 = G(k_0) + m_0$

$y_1 = G(k_1) + m_1$

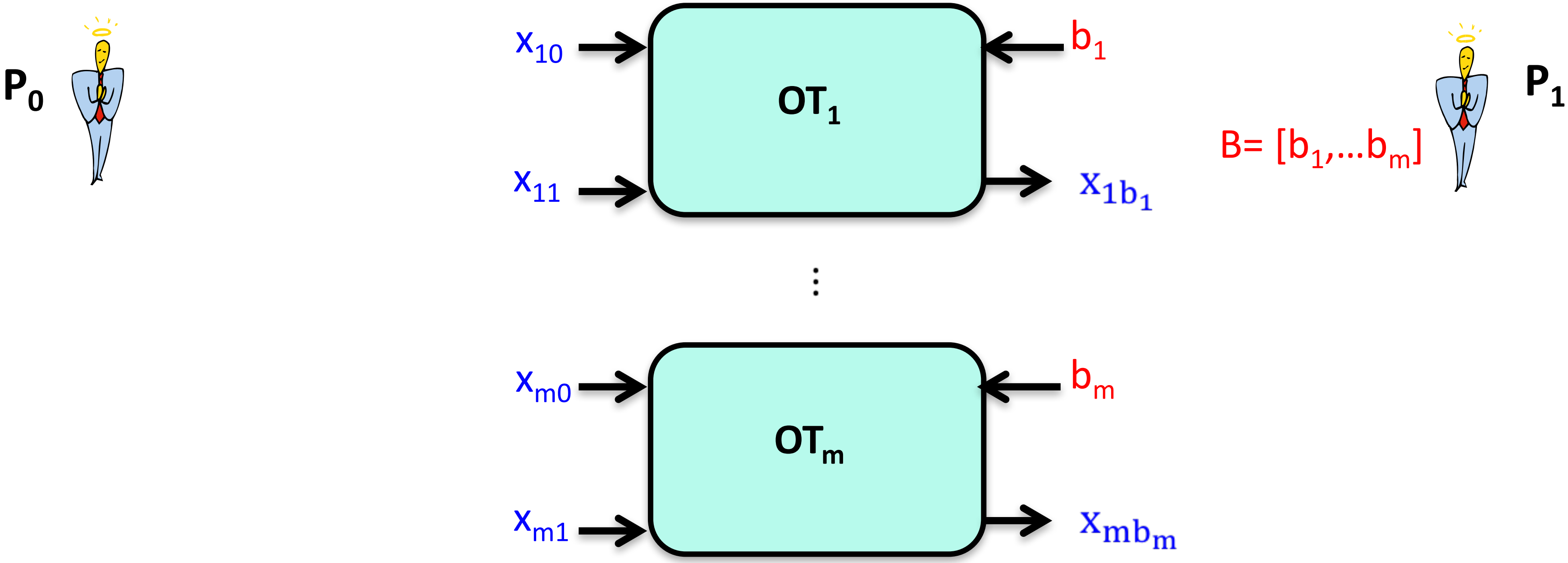
$\xrightarrow{y_0\,,\, y_1}$

$m_b = G(k_b) + y_b$

Roadmap for Building OT Extension [IKNP03]



Transformation II: OT Extension



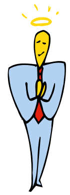
$$Q = \begin{pmatrix} Q_1 = T_1 \text{ (if } b_1 = 0) \ / \ T_1 + S \text{ (otherwise)} \\ Q_2 = T_2 \text{ (if } b_2 = 0) \ / \ T_2 + S \text{ (otherwise)} \\ \\ Q_m = T_m \text{ (if } b_m = 0) \ / \ T_m + S \text{ (otherwise)} \end{pmatrix}$$

$$T = \begin{pmatrix} T_1 \\ T_2 \\ . \\ T_m \end{pmatrix}$$

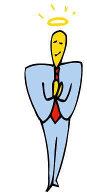
Random S is known to P_0 only

$|T_i| = k$

Transformation II: OT Extension

P_0 

There's a Bug!

 P_1

x_{10}
x_{11}
x_{20}
x_{21}

x_{m0}
x_{m1}

$$Q = \begin{pmatrix} Q_1 = T_1 \text{ (if } b_1 = 0) \;/\; T_1 + S \text{ (otherwise)} \\ Q_2 = T_2 \text{ (if } b_2 = 0) \;/\; T_2 + S \text{ (otherwise)} \\ Q_m = T_m \text{ (if } b_m = 0) \;/\; T_m + S \text{ (otherwise)} \end{pmatrix}$$

$B = [b_1, \ldots b_m]$

$$T = \begin{pmatrix} T_1 \\ T_2 \\ . \\ T_m \end{pmatrix}$$

$y_{10} = Q_1 + x_{10}$

$y_{11} = Q_1 + S + x_{11}$

$y_{m0} = Q_m + x_{m0}$

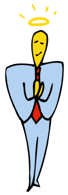
$y_{m1} = Q_m + S + x_{m1}$

$$\xrightarrow{(y_{10}, y_{11}) \ldots\ldots (y_{m0}, y_{m1})}$$

$x_{1\,b1} = T_1 + y_{1\,b1}$

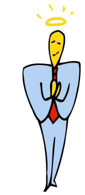
$x_{m\,bm} = T_m + y_{m\,bm}$

Transformation II: OT Extension

P_0 

Given random and independent S, $T_1 \ldots.. T_m$, the joint distribution $\{H(T_1 + S), \ldots. H(T_m + S), T_1 \ldots.. T_m\}$ must be pseudo-random

Cryptographic Hash function: SHA 1/2/3, RC4

 P_1

$B = [b_1, \ldots b_m]$

x_{10}
x_{11}
x_{20}
x_{21}
x_{m0}
x_{m1}

$$Q = \begin{pmatrix} Q_1 = T_1 \text{ (if } b_1 = 0) \ / \ T_1 + S \text{ (otherwise)} \\ Q_2 = T_2 \text{ (if } b_2 = 0) \ / \ T_2 + S \text{ (otherwise)} \\ Q_m = T_m \text{ (if } b_m = 0) \ / \ T_m + S \text{ (otherwise)} \end{pmatrix}$$

$$T = \begin{bmatrix} T_1 \\ T_2 \\ . \\ T_m \end{bmatrix}$$

$y_{10} = H(1, Q_1) + x_{10}$

$y_{11} = H(1, Q_1 + S) + x_{11}$

$x_{1\ b1} = H(1, T_1) + y_{1\ b1}$

$(y_{10}, y_{11}) \ldots\ldots. (y_{m0}, y_{m1})$

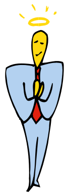
$y_{m0} = H(m, Q_m) + x_{m0}$

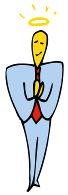
$y_{m1} = H(m, Q_m + S) + x_{m1}$

$x_{m\ bm} = H(m, T_m) + y_{m\ bm}$

Correlation Robust H: $[m] \times \{0,1\}^k \to \{0,1\}^l$

Transformation II: OT Extension

P_0 

 P_1

x_{10}
x_{11}
x_{20}
x_{21}

x_{m0}
x_{m1}

$B = [b_1, \ldots b_m]$

$x_{1\ b1}$

$x_{2\ b2}$

$x_{m\ bm}$

$$Q = \begin{pmatrix} Q_1 = T_1 \text{ (if } b_1 = 0) \ / \ T_1 + S \text{ (otherwise)} \\ Q_2 = T_2 \text{ (if } b_2 = 0) \ / \ T_2 + S \text{ (otherwise)} \\ Q_m = T_m \text{ (if } b_m = 0) \ / \ T_m + S \text{ (otherwise)} \end{pmatrix}$$

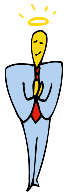
$$T = \begin{pmatrix} T_1 \\ T_2 \\ . \\ T_m \end{pmatrix}$$

Random S is known to P_0 only

$|T_i| = k$

Transformation II: OT Extension

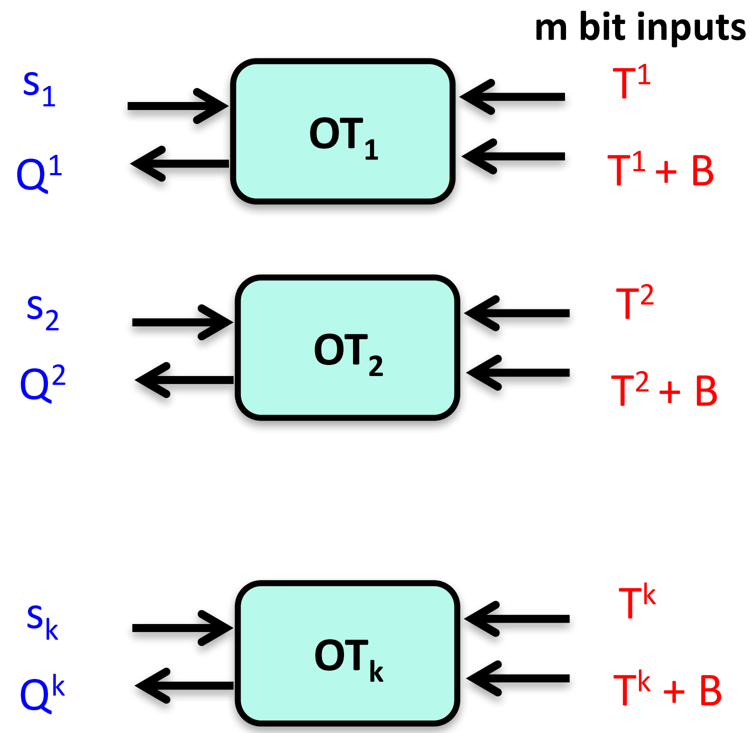
P_0



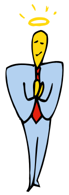
x_{10}
x_{11}
x_{20}
x_{21}

x_{m0}
x_{m1}

Q is a $\{0,1\}^{m.k}$ matrix
$Q = [Q^1 , ...Q^k]$
$$Q=\begin{pmatrix} Q_1 \\ Q_2 \\ . \\ Q_m \end{pmatrix}$$



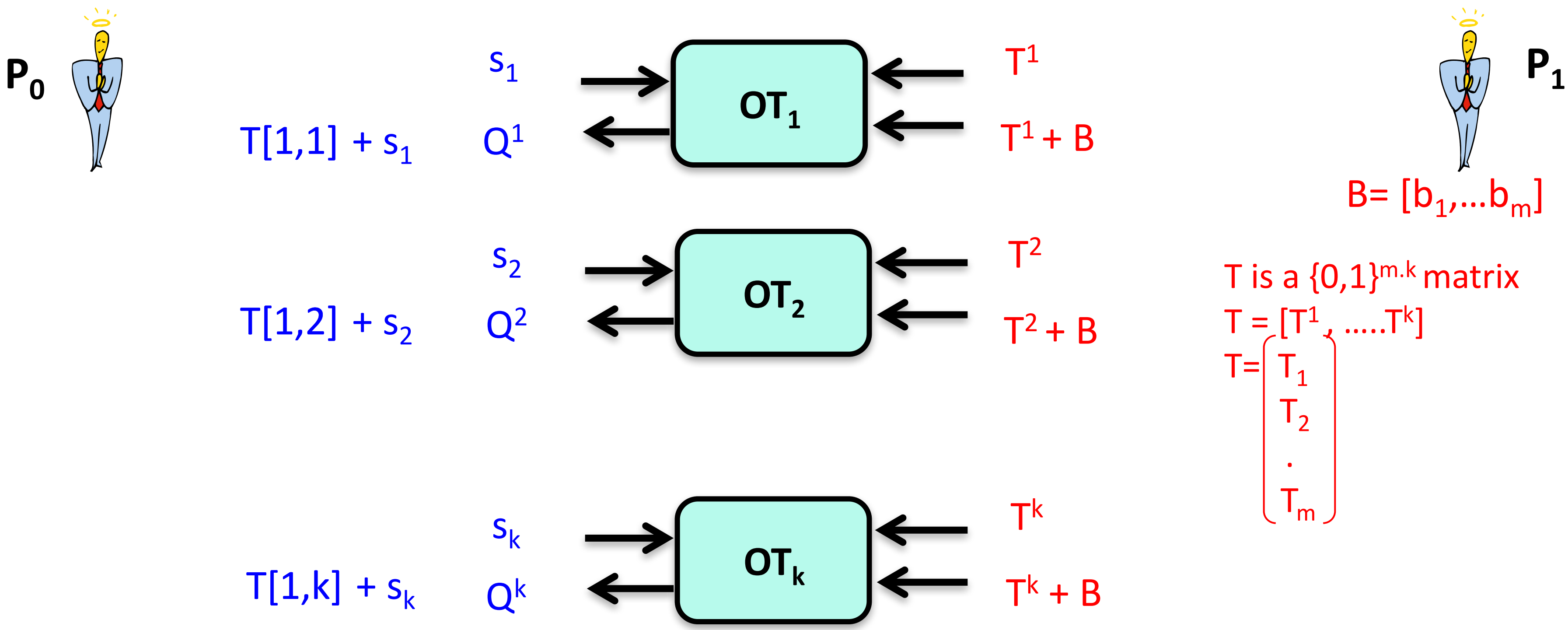
P_1



$B= [b_1,...b_m]$

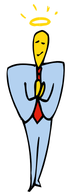
T is a $\{0,1\}^{m.k}$ matrix
$T = [T^1 , ...T^k]$
$$T=\begin{pmatrix} T_1 \\ T_2 \\ . \\ T_m \end{pmatrix}$$

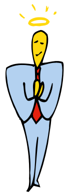
Transformation II: OT Extension



$$Q = \begin{pmatrix} Q_1 = T_1 \text{ (if } b_1 = 0) \;/\; T_1 + S \text{ (otherwise)} \\ Q_2 = T_2 \text{ (if } b_2 = 0) \;/\; T_2 + S \text{ (otherwise)} \\ \\ Q_m = T_m \text{ (if } b_m = 0) \;/\; T_m + S \text{ (otherwise)} \end{pmatrix}$$

Transformation II: Putting everything together

P_0 

 P_1

$B = [b_1, \ldots b_m]$

$s_1 \rightarrow$ **OT_1** $\leftarrow T^1$

$Q^1 \leftarrow$ **OT_1** $\leftarrow T^1 + B$

$s_2 \rightarrow$ **OT_2** $\leftarrow T^2$

$Q^2 \leftarrow$ **OT_2** $\leftarrow T^2 + B$

$s_k \rightarrow$ **OT_k** $\leftarrow T^k$

$Q^k \leftarrow$ **OT_k** $\leftarrow T^k + B$

x_{10}
x_{11}
x_{20}
x_{21}
x_{m0}
x_{m1}

Q is a $\{0,1\}^{m.k}$ matrix
$Q = [Q^1, \ldots .. Q^k]$
$Q = \begin{pmatrix} Q_1 \\ Q_2 \\ . \\ Q_k \end{pmatrix}$

T is a $\{0,1\}^{m.k}$ matrix
$T = [T^1, \ldots .. T^k]$
$T = \begin{pmatrix} T_1 \\ T_2 \\ . \\ T_k \end{pmatrix}$

$y_{10} = H(1, Q_1) + x_{10}$

$y_{11} = H(1, Q_1 + S) + x_{11}$

$x_{1\ b1} = H(1, T_1) + y_{1\ b1}$

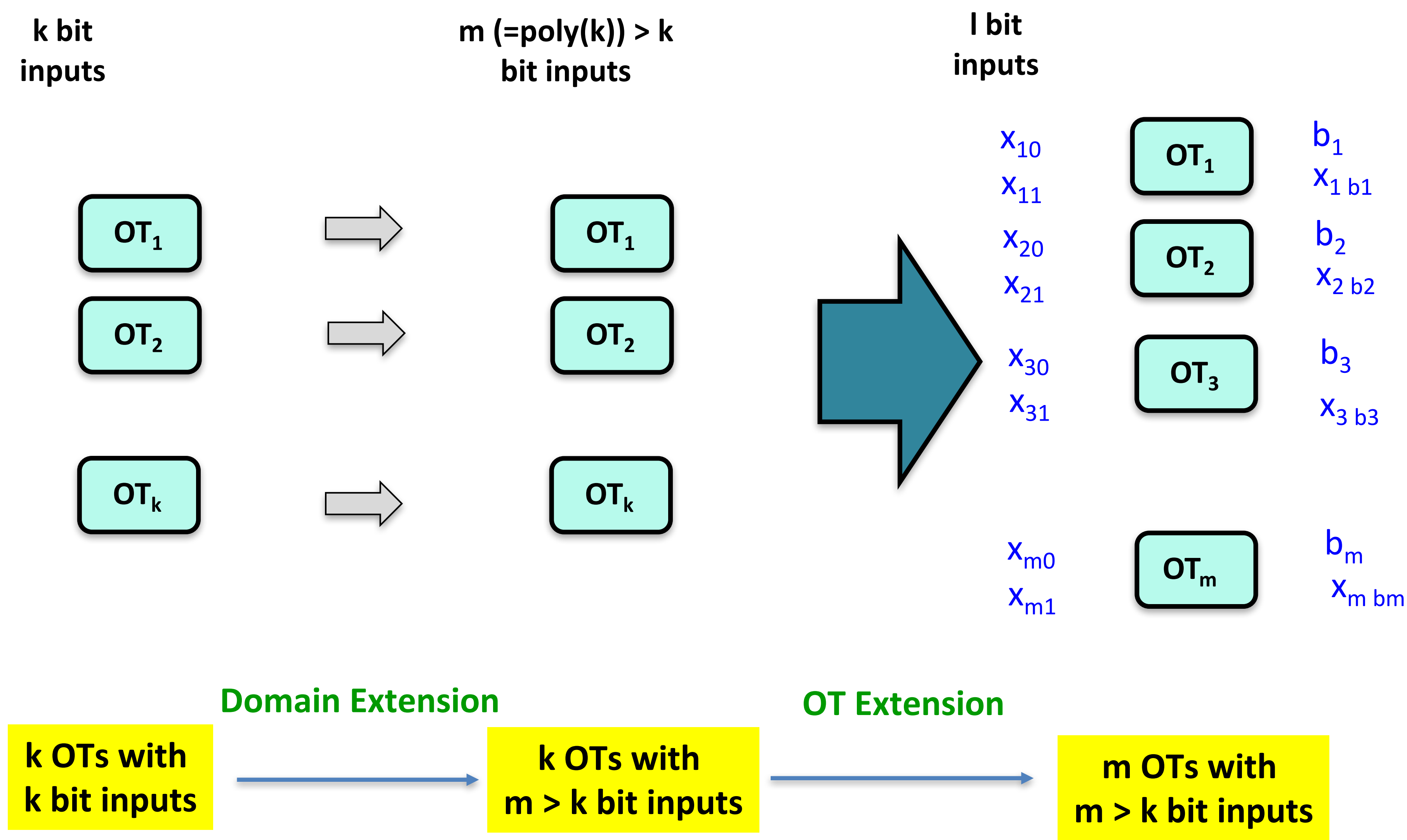
$$\xrightarrow{(y_{10}, y_{11}) \ldots\ldots (y_{m0}, y_{m1})}$$

$y_{m0} = H(m, Q_m) + x_{m0}$

$y_{m1} = H(1, Q_m + S) + x_{m1}$

$x_{m\ bm} = H(m, T_m) + y_{m\ bm}$

Roadmap for Building OT Extension [IKNP03]



Security For Receiver

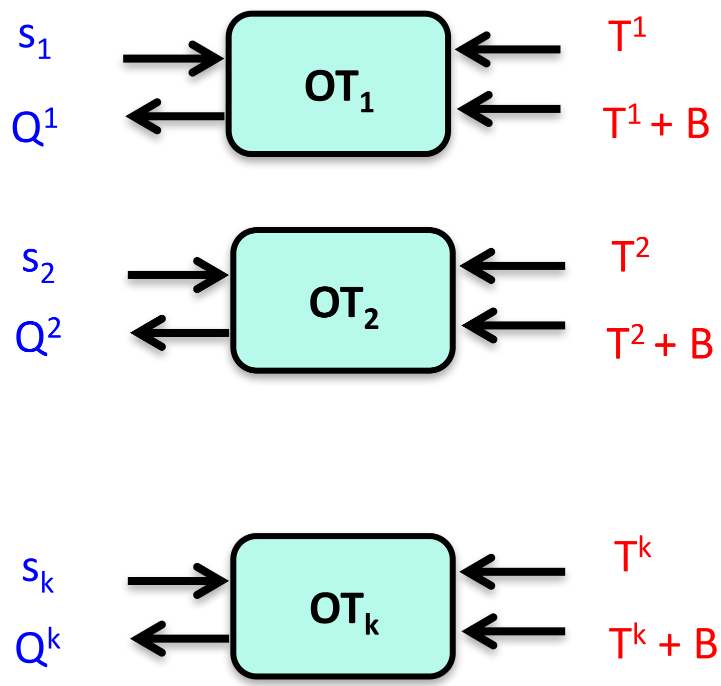
P_0

x_{10}
x_{11}
x_{20}
x_{21}
.
x_{m0}
x_{m1}

Q is a $\{0,1\}^{m.k}$ matrix

$Q = [Q^1, \ldots Q^k]$

$$Q = \begin{pmatrix} Q_1 \\ Q_2 \\ . \\ Q_k \end{pmatrix}$$



P_1

$B= [b_1,\ldots b_m]$

T is a $\{0,1\}^{m.k}$ matrix

$T = [T^1, \ldots T^k]$

$$T = \begin{pmatrix} T_1 \\ T_2 \\ . \\ T_k \end{pmatrix}$$

$y_{10} = H(1,Q_1) + x_{10}$

$y_{11} = H(1,Q_1 + S) + x_{11}$

$y_{m0} = H(m,Q_m) + x_{m0}$

$y_{m1} = H(1,Q_m + S) + x_{m1}$

Reduces to the sender's security of $OT_1 \ldots OT_k$

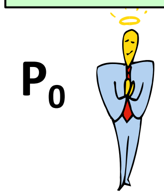
$(y_{10}, y_{11}) \ldots\ldots (y_{m0}, y_{m1})$

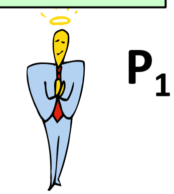
$x_{1\ b1} = H(1,T_1) + y_{1\ b1}$

$x_{m\ bm} = H(m,T_m) + y_{m\ bm}$

Security For Sender

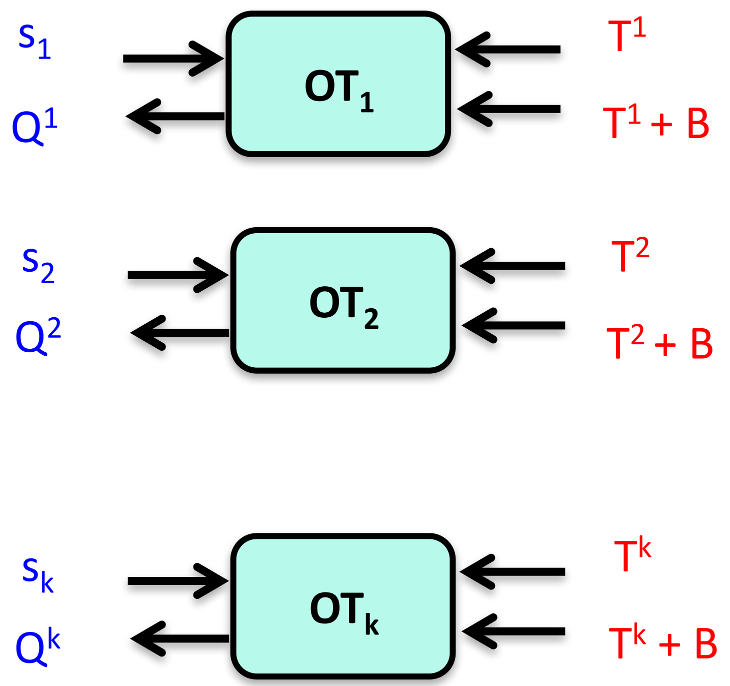
[IKNP03]: Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In CRYPTO ,pages 145–161, 2003.





x_{10}
x_{11}
x_{20}
x_{21}
x_{m0}
x_{m1}

Q is a $\{0,1\}^{m.k}$ matrix
$Q = [Q^1, \ldots.. Q^k]$
$Q = \begin{pmatrix} Q_1 \\ Q_2 \\ . \\ Q_k \end{pmatrix}$



$B = [b_1, \ldots b_m]$

T is a $\{0,1\}^{m.k}$ matrix
$T = [T^1, \ldots.. T^k]$
$T = \begin{pmatrix} T_1 \\ T_2 \\ . \\ T_k \end{pmatrix}$

$y_{10} = H(1,Q_1) + x_{10}$

$y_{11} = H(1,Q_1 + S) + x_{11}$

Reduces to the receiver's security of OT_1 …OT_k

$x_{1\ b1} = H(1,T_1) + y_{1\ b1}$

$(y_{10}, y_{11}) \ldots\ldots (y_{m0}, y_{m1})$

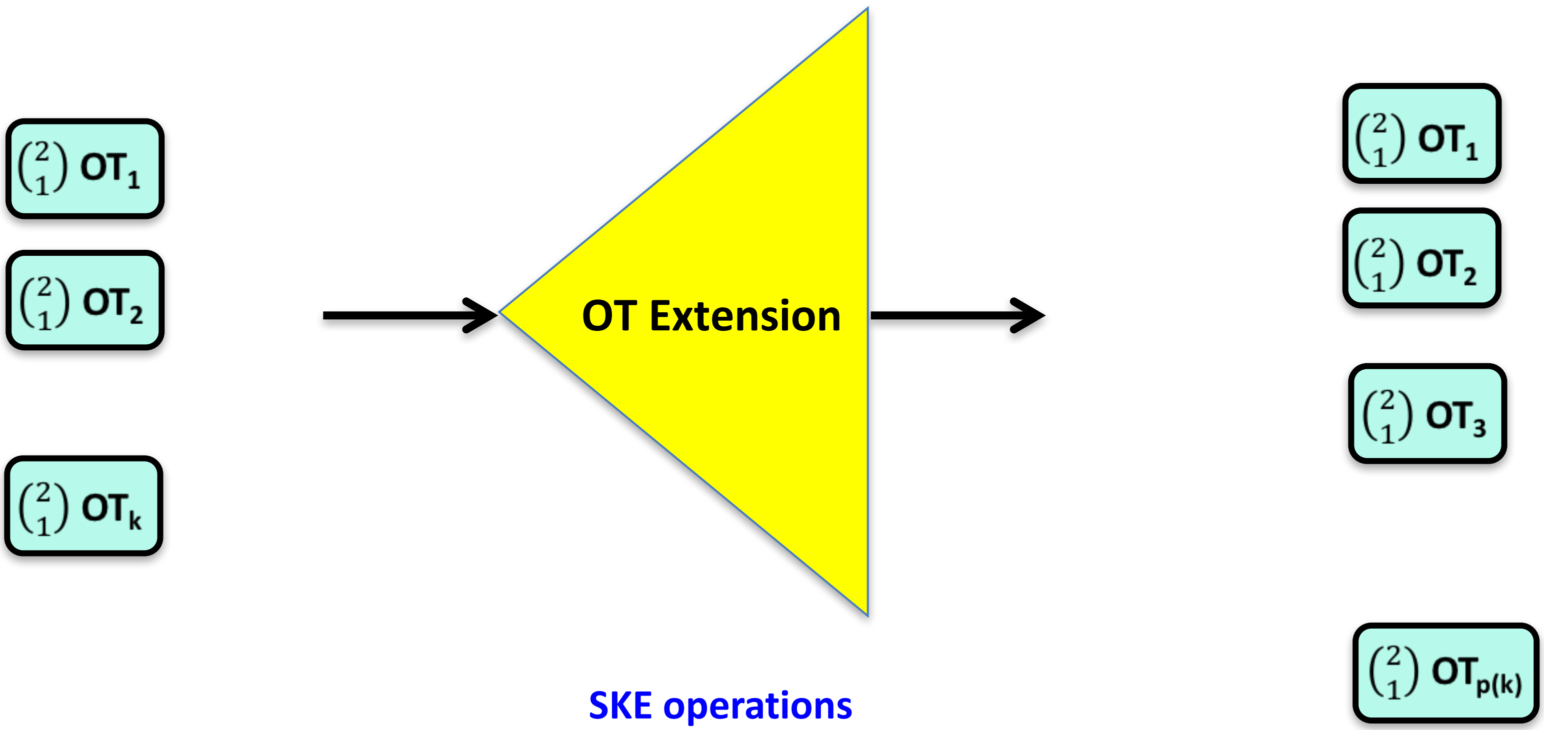
$y_{m0} = H(m,Q_m) + x_{m0}$

$y_{m1} = H(1,Q_m + S) + x_{m1}$

Reduces to the security of H

$x_{m\ bm} = H(m,T_m) + y_{m\ bm}$

IKNP and Its Successors

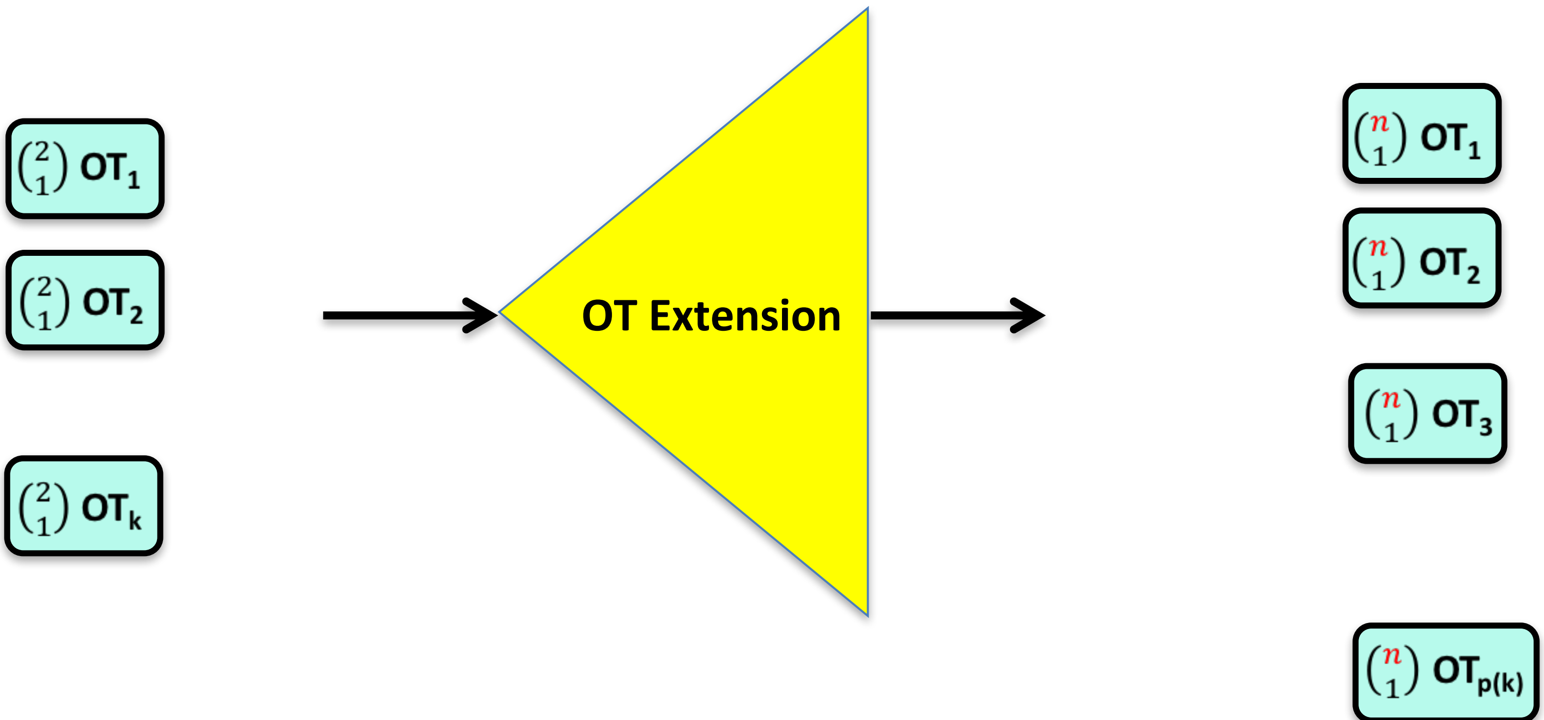


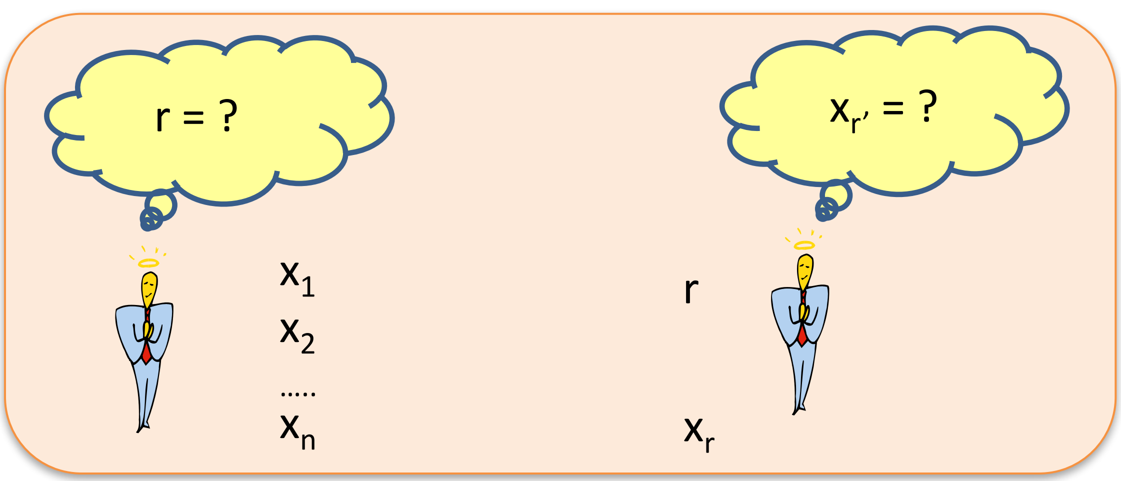
Semi-honest: IKNP, ALSZ13

Active: NNOB, ALSZ15,KOS15

k: security parameter

KK13 and Its Successors





Used in PSI, PIR etc

Semi-honest: KK13

Active: PSS17, OOS17

k: security parameter

OT Study Group

The list will be updated as and when needed.

| Basic Definitions & Reductions | Meeting 1 (18.05.15; 11am -1pm) | **Leaders: Abhishek, Ajith, Priyanka** |

- 1-out-of-2 OT, Rabin OT, equivalence: [Ost_LN],[Cramer_LN], [Crepeau87]
- 1-out-of-n OT, k-out-of-n OT, Reduction to 1-out-of-2 OT [Katz_LN],[Cramer_LN]
- Reducing 1-out-of-2 OT to Random OT: [WW06], [Lin09],[Katz_LN]
- Symmetricity of 1-out-of-2 OT: [WW06]

| Various Security Notions | Meeting 2 (22.05.15; 3:30 - 5:50 pm),3 (25.05.15; 3:30 - 5:50 pm),4 (27.05.15; 3:30 - 5:50 pm) | **Leaders: Dheeraj, Divya, Kuljeet** |

- Privacy only Security & Constructions: Hazay & Lindell
- One-sided Simulation & Constructions: Hazay & Lindell
- Full Simulation & Constructions: Hazay & Lindell

| OT from Generic Assumptions | Meeting 5 (29.05.15; 3:30 - 5:50 pm) | **Leaders: Ajith, Anchita** |

- OT from Enhanced TDF/ CPA-secure PKE with PK samplability (EGL): Chapter 3 of [Rothblum], [Katz_LN1],[Katz_LN2], Section 2 of [Hai08]
- OT from Homomorphic Encryption: Hazay & Lindell

| OT Extensions | Meeting 6 (09.06.15; 3:30 - 5:50 pm),7 (11.06.15; 3:30 - 5:50 pm) ,8 (12.06.15; 3:30 - 5:50 pm) | **Leaders: Ajith, Dheeraj, Divya, Kuljeet** |

Updates

NEW Updated list of

Introduction

Indocrypt 2017 is the 18th International Conference on Cryptology in India. The conference will take place during 10-13 December 2017 at The Institute of Mathematical Sciences (IMSc), Chennai. Indocrypt 2017 is part of the Indocrypt series organized under the aegis of the Cryptology Research Society of India.

Important Dates

- Paper Submission Deadline : Aug 20 (12.00 GMT)
- Notification of Acceptance: Oct 5
- Final Manuscripts Due : Oct 15
- **Conference: 10-13 December 2017**

General chairs

C. Pandu Rangan
Indian Institute of Technology Madras, India

R. Balasubramanian
Institute of Mathematical Sciences, India

Program chairs

Arpita Patra
Indian Institute of Science, India

Nigel P. Smart
University of Bristol, UK

Sponsors/Co-organizers

In cooperation with

Thank You!

OT Extension- Recent Advances

[KK13]: From k 1-out-2 OTs to m 1-out-of-n OTs

Most efficient in semi-honest setting

Uses Walsh-Hadamard Code

Semi-honest

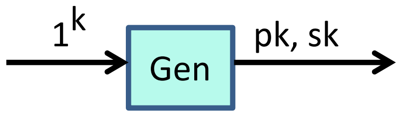
[KOS15]: Most efficient maliciously secure IKNP

[PSS17]: Most efficient maliciously secure KK13

Active/Malicious

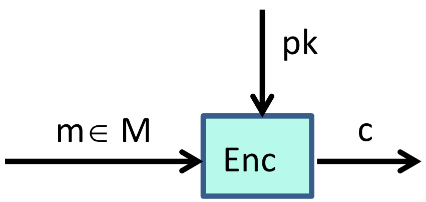
OT from CPA-secure PKE with Public Key Samplability [EvenGoldreichLempel85]

A public-key encryption scheme is a collection of 3 PPT algorithms Π = (Gen, Enc, Dec)



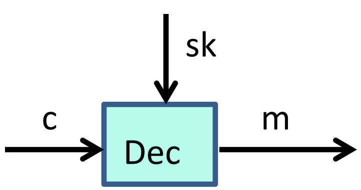
Syntax: $(pk, sk) \leftarrow Gen(1^k)$

Randomized Algo



Syntax: $c \leftarrow Enc_{pk}(m)$

Randomized algo



Syntax: $m := Dec_{sk}(c)$

Deterministic (w.l.o.g)

Except with a negligible probability over (pk, sk) output by $Gen(1^k)$, we require the following for every (legal) plaintext m

$Dec_{sk}(Enc_{pk}(m)) := m$

CPA Security

Indistinguishability experiment $\mathrm{PubK}^{\mathrm{cpa}}_{A,\Pi}(k)$

n, Enc, Dec)

In the real-world, everyone including the attacker will have the public key pk

PPT A

I can break Π

pk

$m_0, m_1, |m_0|=|m_1|$

$c \leftarrow \mathrm{Enc}_{pk}(m_b)$

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

(Attacker's guess about encrypted message)

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

Let me verify

pk, sk

$\mathrm{Gen}(1^k)$

Game Output

$b = b'$

1 --- attacker won

$b \neq b'$

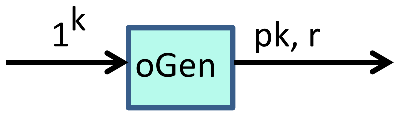
0 --- attacker lost

Π is CPA-secure if for every PPT attacker A taking part in the above experiment, the probability that A wins the experiment is at most negligibly better than ½

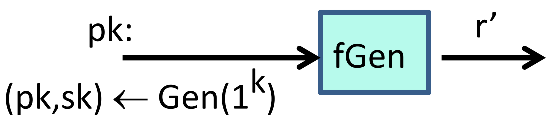
$$\Pr\left(\mathrm{PubK}^{\mathrm{cpa}}_{A,\Pi}(k) = 1\right) \leq \frac{1}{2} + \mathrm{negl}(k)$$

PKE with Public Key Samplability

A public-key encryption scheme is a collection of 5 PPT algorithms Π = (Gen, Enc, Dec, oGen, fGen)



Syntax: (pk, r) $\leftarrow$ oGen(1^k)



Syntax: r’ $\leftarrow$ fGen(pk)

(pk,r’) and (pk,r) look indistinguishable

Key Samplability

Indistinguishability experiment $\mathrm{PubK}^{\mathrm{ksamp}}_{A,\Pi}(k)$

Π = (Gen, Enc, Dec, oGen, fGen)

PPT A

I can break Π

(pk,r)

b' $\in$ {0, 1}

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

(pk, sk) $\leftarrow$Gen(1^k)

r $\leftarrow$fGen(pk)

(pk, r) $\leftarrow$oGen(1^k)

Game Output

$b = b'$

1 --- attacker won

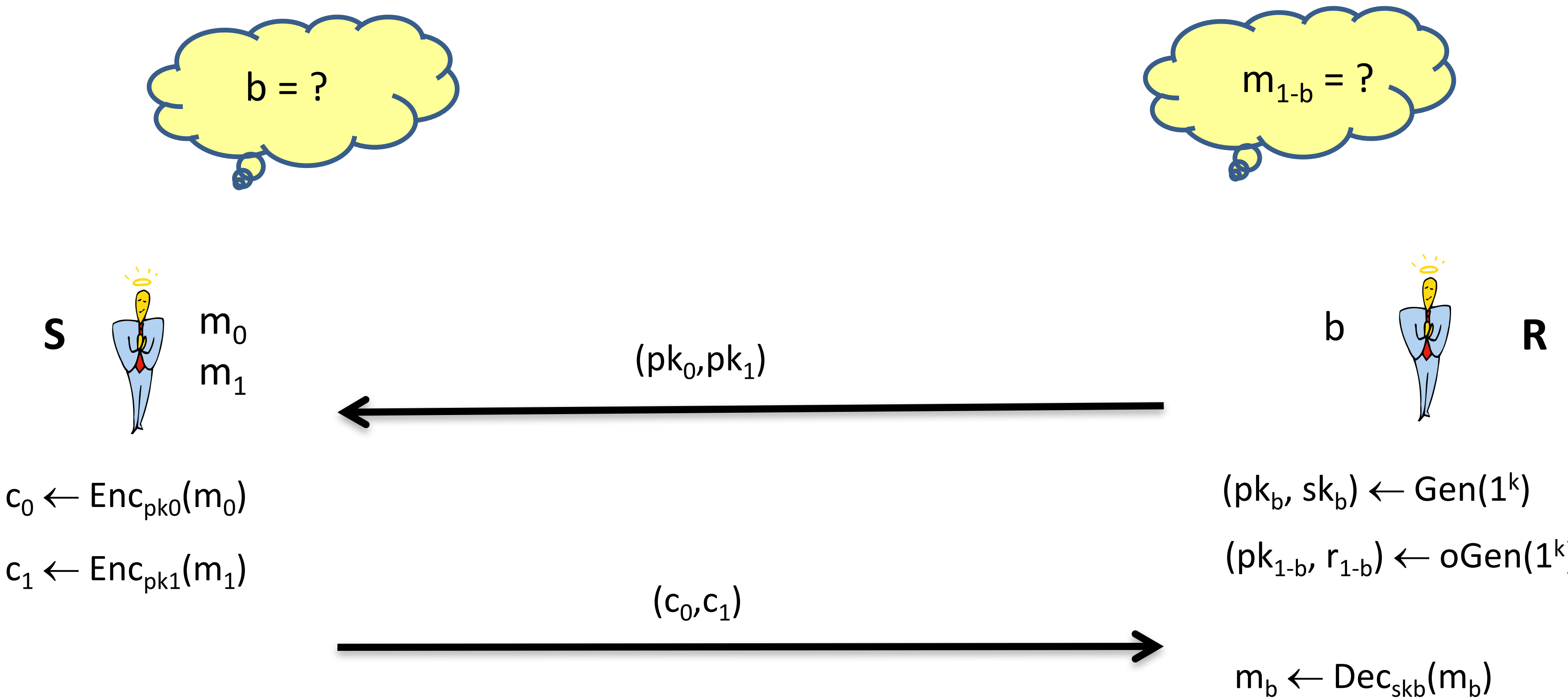
$b \neq b'$

0 --- attacker lost

Π is key-samplable if for every PPT attacker A taking part in the above experiment, the probability that A wins the experiment is at most negligibly better than ½

$$\Pr\left(\mathrm{PubK}^{\mathrm{ksamp}}_{A,\Pi}(k) = 1\right) \leq \frac{1}{2} + \mathrm{negl}(n)$$

1-out-of-2 Oblivious Transfer



- OTs are **intrinsically expensive**- usually based on public key primitives
- AES Circuit: Millions of AND gates

ElGamal PKE

Gen(1^k)

(G, o, q, g)

$h = g^{x}$. For random x

pk= (G,o,q,g,h), sk = x

$\mathrm{Enc}_{pk}(m)$

$c_1 = g^y$ for random y

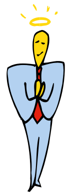
$c_2 = h^{y}$. m

$c = (c_1, c_2)$

$\mathrm{Dec}_{sk}(c)$

$c_2 / (c_1)^x = c_2 \cdot [(c_1)^x]^{-1}$

Transformation II: OT Extension

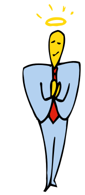
P_0 

Random Oracle

Every time query an input: same output

New input: output is completely random in the range

Every RO is Correlation-Robust (HR) Hash function

 P_1

$B= [b_1,\dots b_m]$

r_{10}

r_{11}

r_{20}

r_{21}

$Q= [Q_1 = T_1$ (if $b_1 = 0$) / $T_1 + S$ (otherwise)

$Q_2 = T_2$ (if $b_2 = 0$) / $T_2 + S$ (otherwise)

$Q_m = T_m$ (if $b_m = 0$) / $T_m + S$ (otherwise)]

r_{m0}

r_{m1}

$T= [T_1$

T_2

.

$T_k]$

$y_{10} = H(1,Q_1) + r_{10}$

$y_{11} = H(1,Q_1 + S) + r_{11}$

$r_{1\ b1} = T_1 + y_{1\ b1}$

$(y_{10}, y_{11})\dots\dots (y_{m0}, y_{m1})$

$y_{m0} = H(m,Q_m) + r_{m0}$

$y_{m1} = H(m,Q_m + S) + r_{m1}$

$r_{m\ bm} = T_m + y_{m\ bm}$

Random Function H: $[m] \times \{0,1\}^k \to \{0,1\}^l$

A little diversion to RO Model

>> Love and hate relationship with this model

>> Many protocols have proof in RO model which otherwise does not have any proof.

>> Real protocol: RO replaced with hash functions

>> Protocol analyzed for Security: Hash functions replaced with RO box.

>> Proof is for any good?: Existence of such a proof implies the real protocol go wrong only when hash function does not simulate RO. Some proof better than no proof

>> Examples: RSA-OEAP (practically in use). CCA-secure extension of RSA

>> Finding proof under relatively realistic assumption (e.g. CR) than RO has been very challenging and considered to be great achievement!!

Random Function H: $[m] \times \{0,1\}^k \rightarrow \{0,1\}^l$