CSE 539: Applied Cryptography
Week 13: Oblivious Transfer

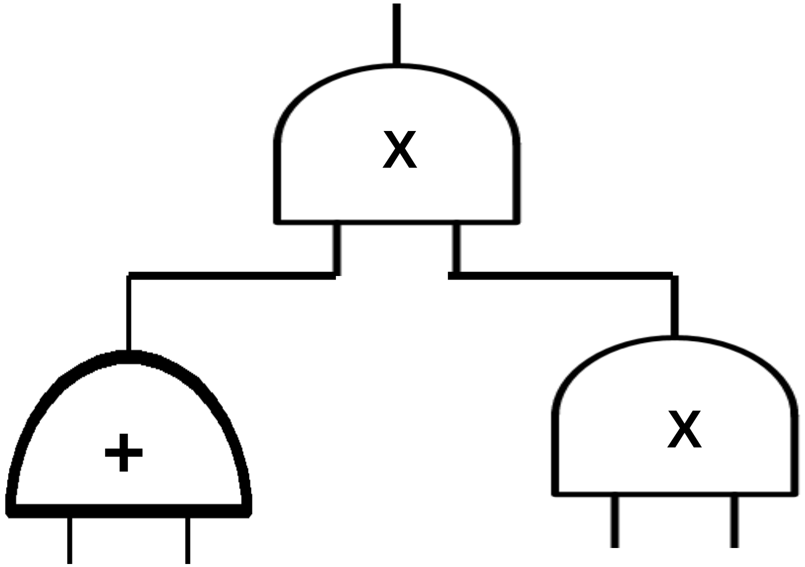
Ni Trieu (ASU)

Reading:

- https://web.engr.oregonstate.edu/~rosulekm/cryptabit/1-overview.pdf
- https://securecomputation.org/docs/ch1-introduction.pdf
- https://securecomputation.org/docs/ch2-definingmpc.pdf

Recap: Secure Computation

- Secure computation is a magic box
  - Yao’s Protocol (Garbled Circuit)



Recap: Yao’s Protocol

x > y ?

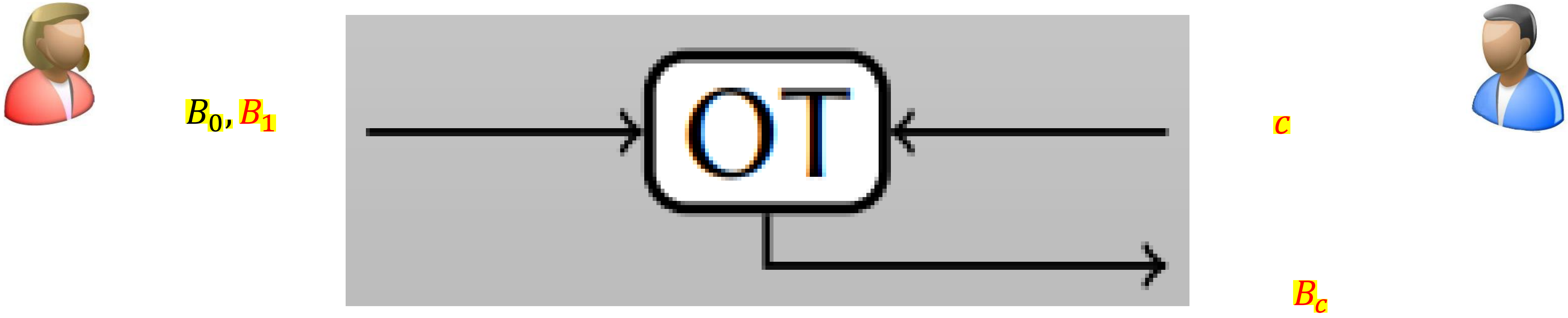
- Input domain: $x, y \in \{1,2\}$
  - Alice’s input: $x = 1$
  - Bob’s input: $y = 2$
- Strawman solution:
  - Alice does the following :
    - Write truth table of function f$(x, y) = x > y$?
    - For each possible input,
      choose random cryptographic key
    - Encrypt each output with corresponding keys
    - Randomly permute ciphertexts, send to Bob

Somehow Bob obtains only “correct” encrypted keys: A_x, B_y

  - Bob learns only f(x, y)
  - [Informal security]:
    - Alice learns nothing
    - Bob learns A_x, but not x. Bob can only decrypt Enc_{A_x,B_y}(f(x, y))

x	y	$f(x, y)$
A_1	B_1	$Enc_{A_1,B_1}(f(1,1))$
A_2	B_3	$Enc_{A_2,B_3}(f(2,3))$
A_1	B_3	$Enc_{A_1,B_3}(f(1,3))$
A_2	B_1	$Enc_{A_2,B_1}(f(2,1))$
A_2	B_2	$Enc_{A_2,B_2}(f(2,2))$
A_1	B_2	$Enc_{A_1,B_2}(f(1,2))$
A_3	B_1	$Enc_{A_3,B_1}(f(3,1))$
A_3	B_2	$Enc_{A_3,B_2}(f(3,2))$
A_3	B_3	$Enc_{A_3,B_3}(f(3,3))$

Oblivious Transfer Functionality



Oblivious Transfer (OT) refers to the setting where a sender with two input strings (m_0, m_1) interacts with a receiver who has an input choice bit b. As the result, the receiver learns mb without learning anything about m_{1-b}, while the sender learns nothing about b.

Oblivious Transfer Construction

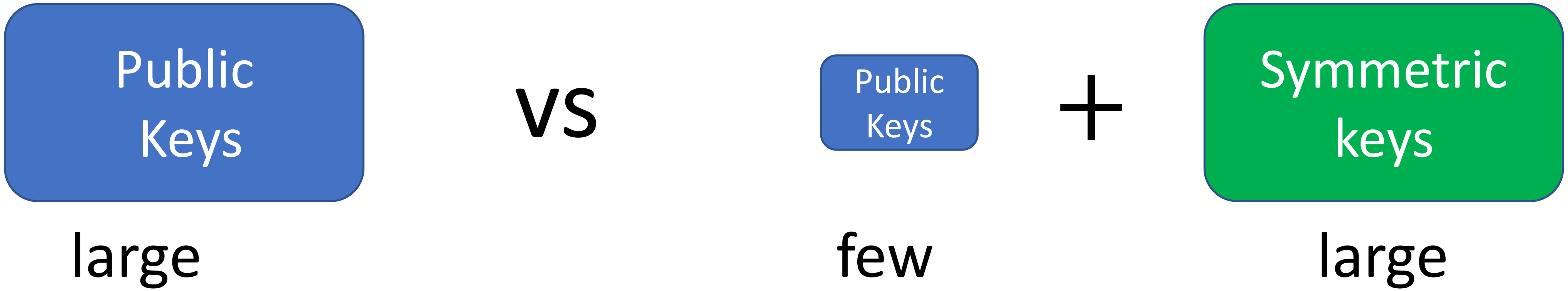
Oblivious Transfer: Security

OBLIVIOUS TRANSFER EXTENSION

[Beaver'96, Ishai-Kilian-Nissim-Petrank'03]

- OT (using PK) is expensive

- Few OTs+ symmetric keys => many OTs [Ishai-Kilian-Nissim-Petrank'03]
  - But still need to communicate $O(\kappa)$ bits per random OT, where κ is security parameter



Public Keys

large

vs

Public Keys

few

+

Symmetric keys

large

Oblivious Transfer Construction (reading)

- https://www.iacr.org/archive/crypto2003/27290145/27290145.pdf
- https://eprint.iacr.org/2013/552.pdf
- https://eprint.iacr.org/2015/061.pdf
- https://eprint.iacr.org/2013/491.pdf
- https://eprint.iacr.org/2019/634.pdf