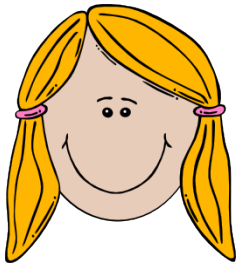
On Invertible Sampling and Adaptive Security

Yuval Ishai – *Technion*
Abishek Kumarasubramanian - *UCLA*
Claudio Orlandi – *Aarhus University*
Amit Sahai - *UCLA*

OT and sampling public keys…



b

m_0, m_1

$pk_b \leftarrow G(sk_b)$

$pk_{1-b} \leftarrow U(r)$

(pk_0, pk_1)

$C_0 \leftarrow E_{pk0}(m_0)$

$C_1 \leftarrow E_{pk1}(m_1)$

(C_0, C_1)

$m_b = D(sk_b, C_b)$

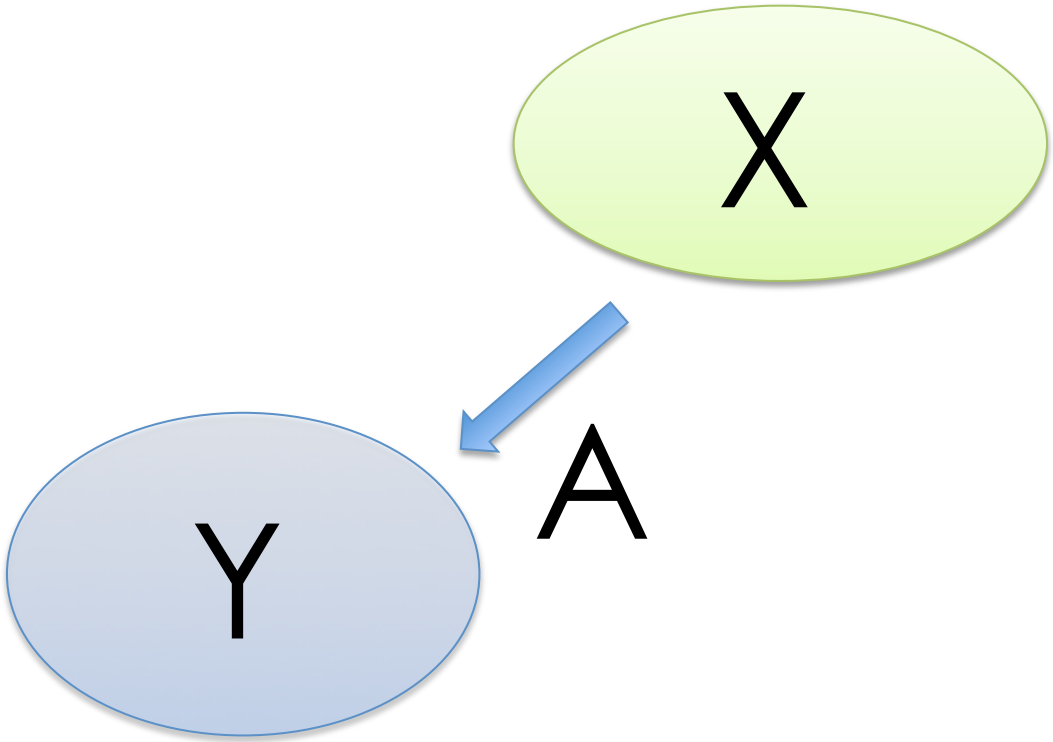
Outline

- Invertible Sampling Hypothesis (ISH)
- ISH is (conditionally) false
- ISH and Adaptive Secure MPC
- General AMPC is impossible

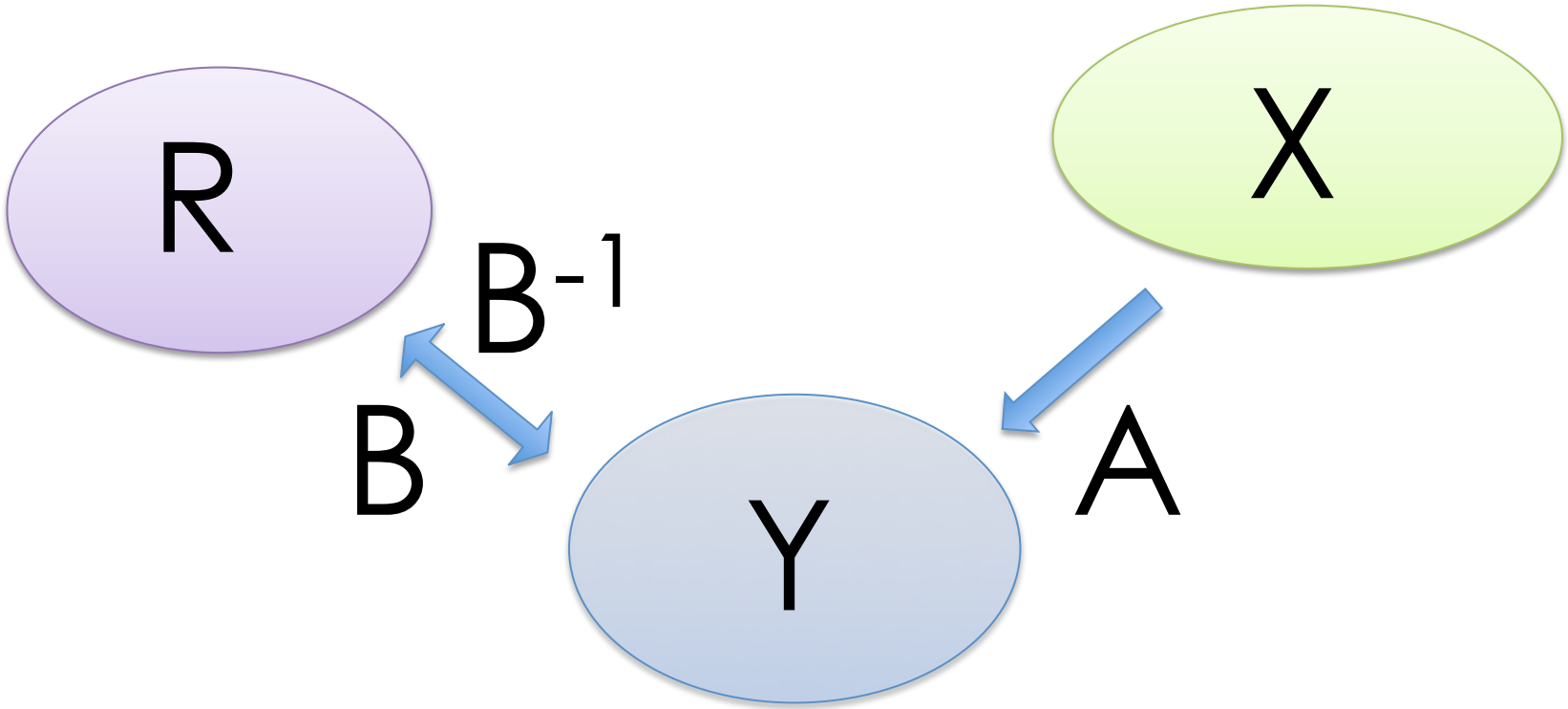
Outline

- Invertible Sampling Hypothesis (ISH)
- ISH is (conditionally) false
- ISH and Adaptive Secure MPC
- General AMPC is impossible

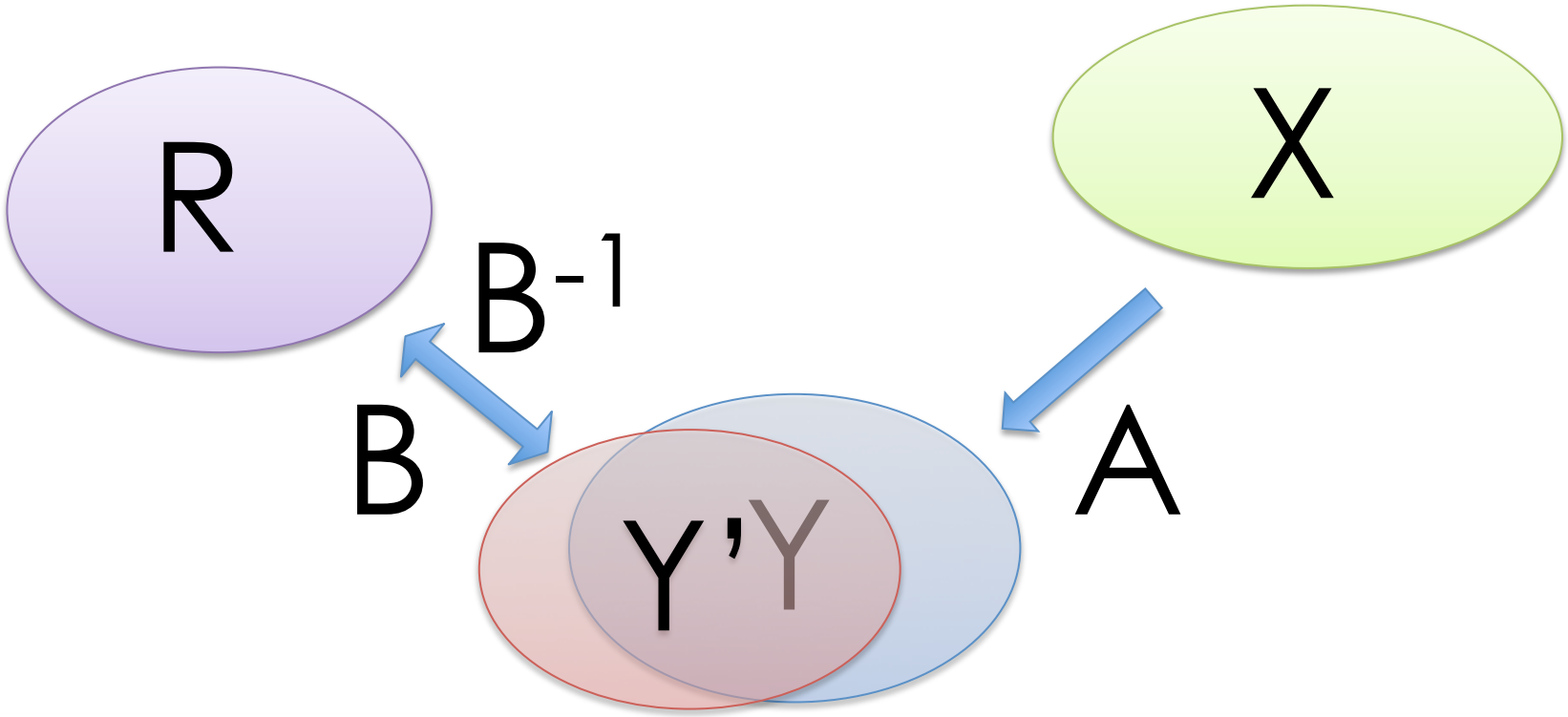
Invertible Sampling



Invertible Sampling



Invertible Sampling



Applications in:

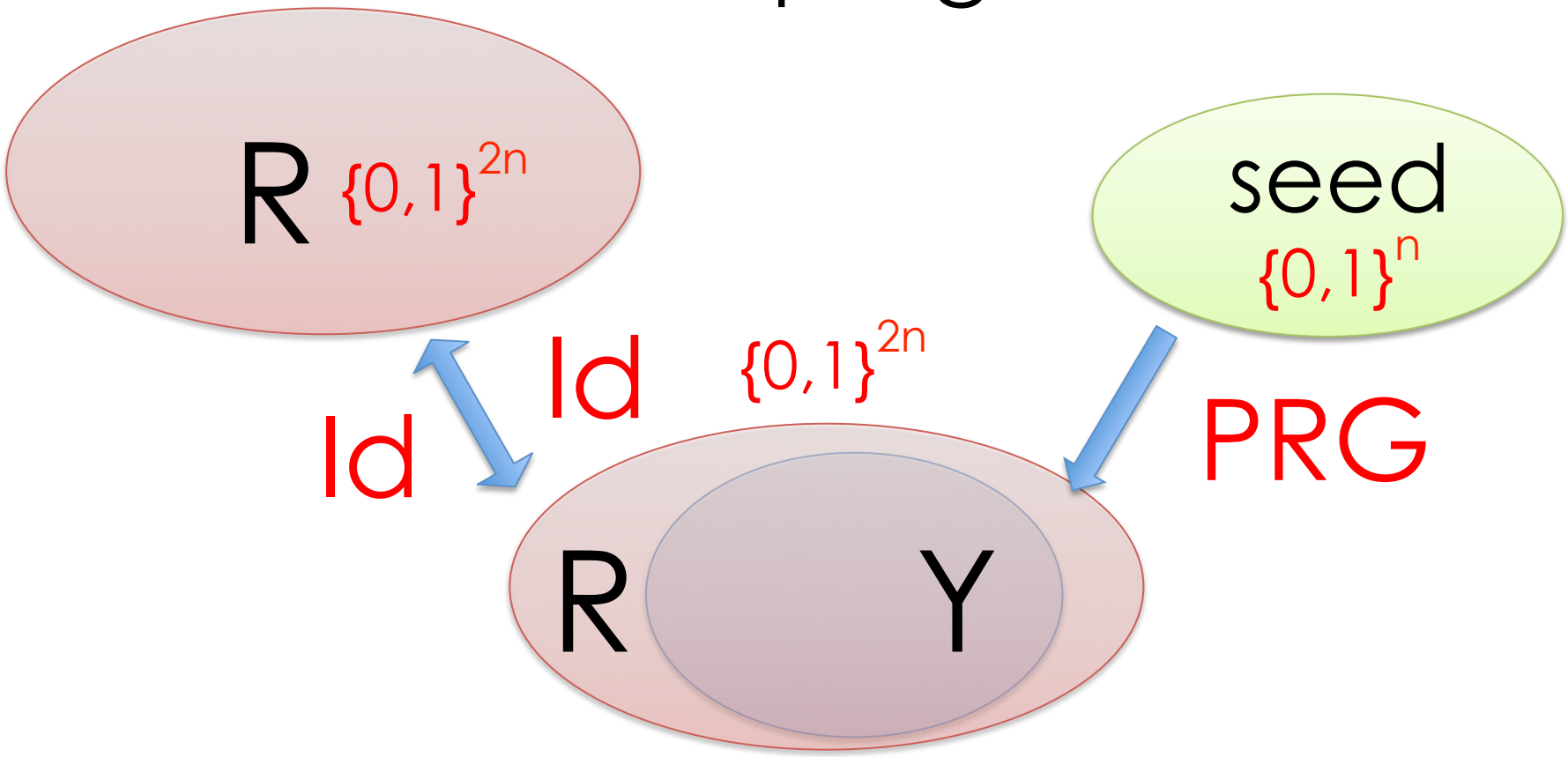
OT, Non-Committing Encryption,

Adaptive Security, UC setup assumptions

Invertible Sampling Hypothesis (ISH)

- For all PPT A there exist B, B^{-1} s.t.
  - The output distributions of A, B are computationally indistinguishable
  - B can be inverted efficiently using B^{-1}

Invertible Sampling of PRG



- PRG/randomness are comp. close
- Identity can be inverted

Outline

- Invertible Sampling Hypothesis (ISH)
- ISH is (conditionally) false
- ISH and Adaptive Secure MPC
- General AMPC is impossible

Knowledge One Way Function
[Canetti-Douk08]

- A function *f* is a Knowledge OWF (KOWF) if it is OWF and, for all PPT *M* there exist a knowledge extractor K_M s.t.: let

$$y \leftarrow M(r), x \leftarrow K_M(r)$$

Then if *y* is in the image of *f* ➔ $y = f(x)$

(except with negligible probability)

Knowledge of Exponent
[Damgård91]

For every adversary M, (g,h) generators of group G s.t.

$$(u,v) \leftarrow M(g,h; r)$$

There is a knowledge extractor K_M

$$x \leftarrow K_M(g,h; r)$$

Such that:

$$If\ (u,v) = (g^w,h^w) \rightarrow x = w$$

Theorem:
If KOWF + NIZK exist
➔ ISH is false

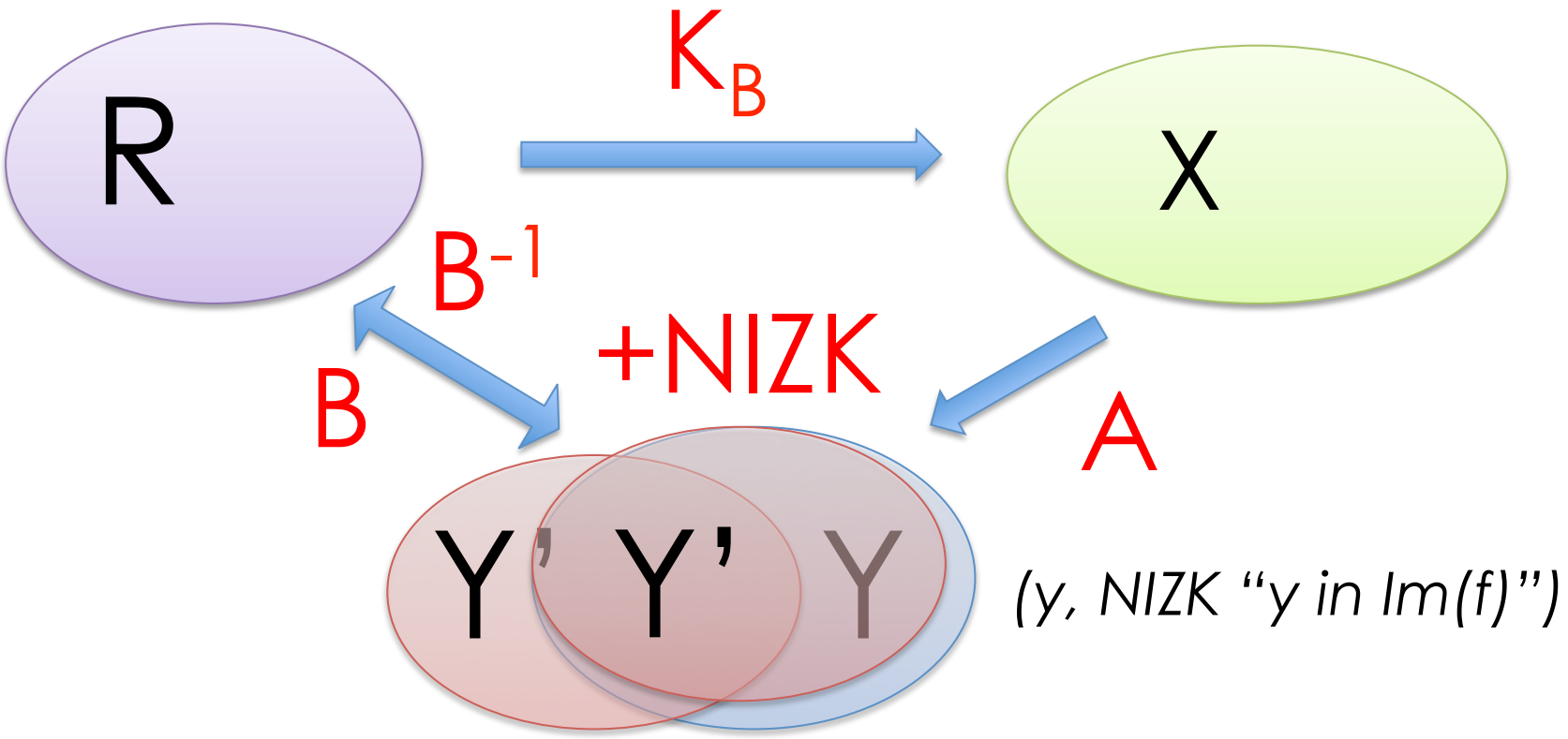
Proof:

Counterexample: *f* is KOWF

(y, NIZK of "y is in Im(f)") ← A(x)

if there are B,B^{-1} (as in ISH), f is not OWF

ISH is false

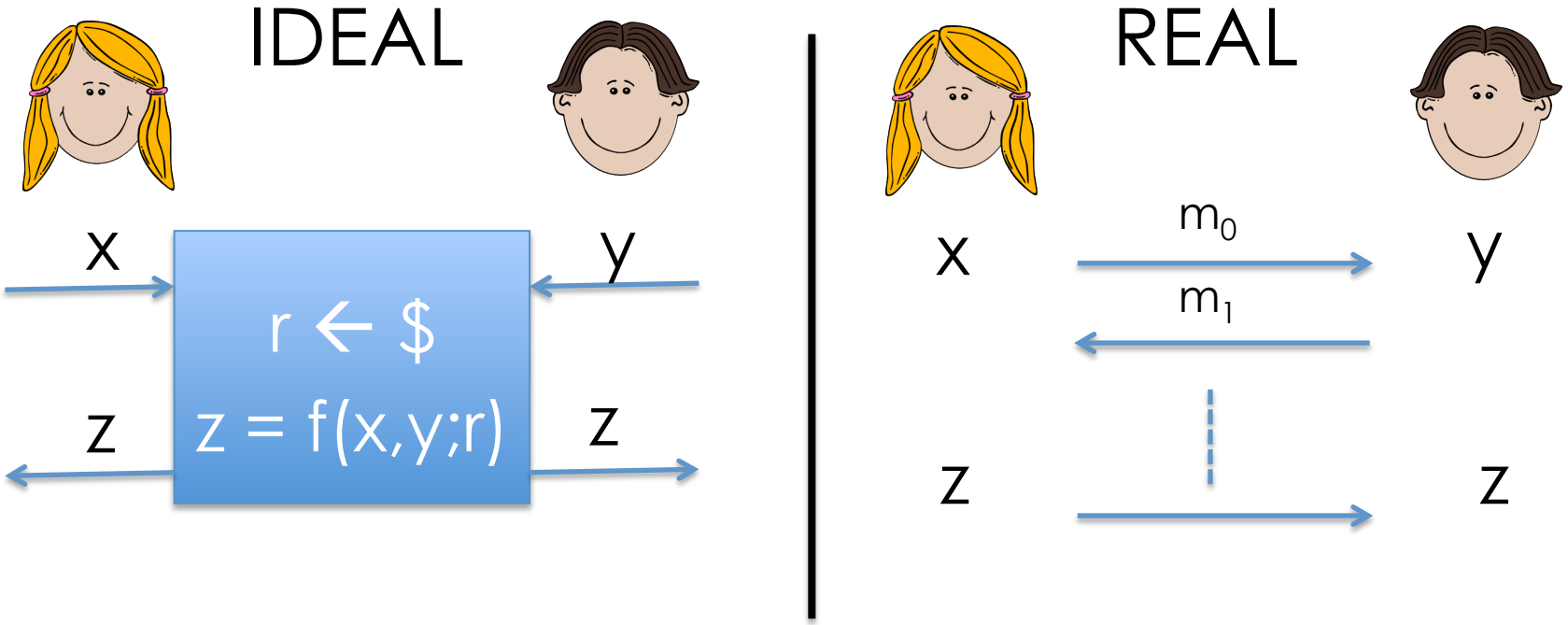


- Y, Y' are statistically close (NIZK)
- Any algorithm that samples from Y has a knowledge extractor (**K**OWF)

Outline

- Invertible Sampling Hypothesis (ISH)
- ISH is (conditionally) false
- ISH and Adaptive Secure MPC
- General AMPC is impossible

Multi Party Computation
(with Adaptive Security)



- The protocol is secure if an adversary that can corrupt parties at any time can be simulated in the ideal world

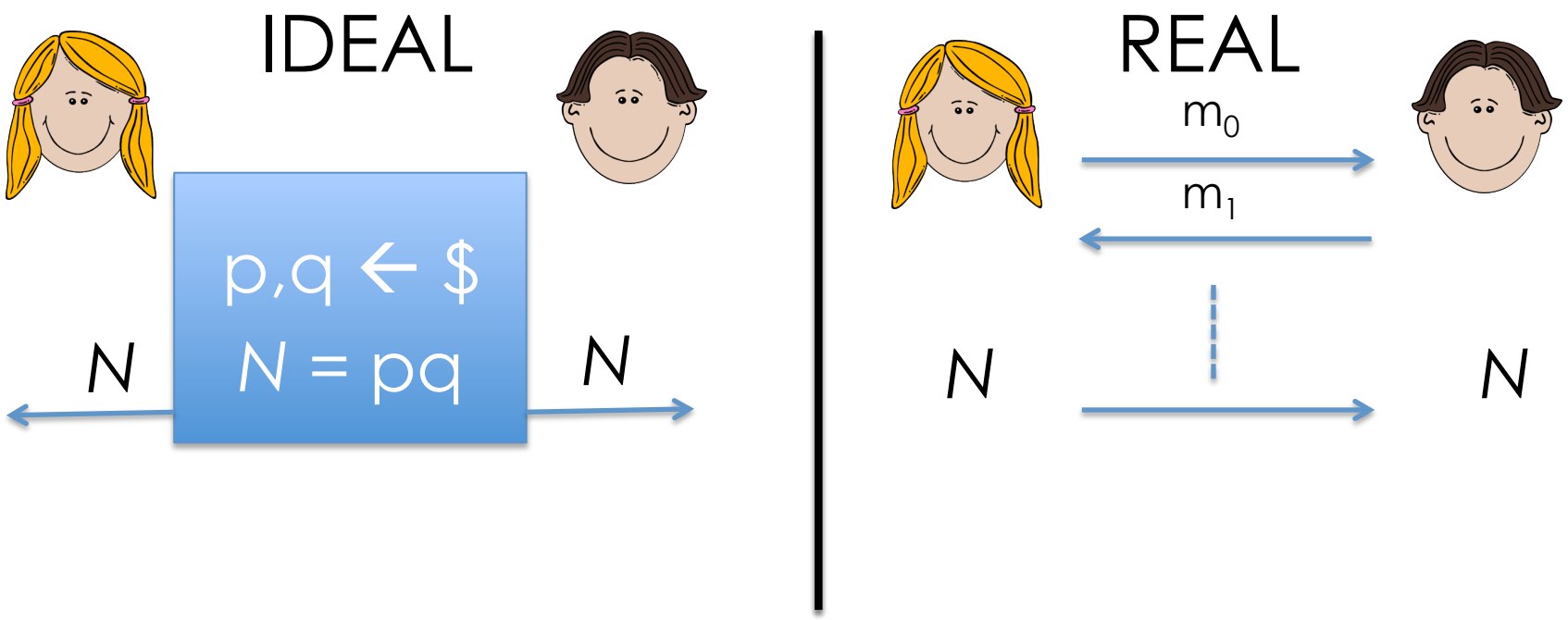
MPC with Adaptive Security

- Adaptive security [CFGN'96]:
  - Strong security model
  - Easier with erasure or with honest majority
  - Difficult to achieve otherwise

- UC AMPC [CLOS'02]
  - Deterministic functionalities can be AMPCed
  - Randomized functionalities, only if well-formed

- Well-formed: technical requirement, about the internal randomness of the ideal functionality

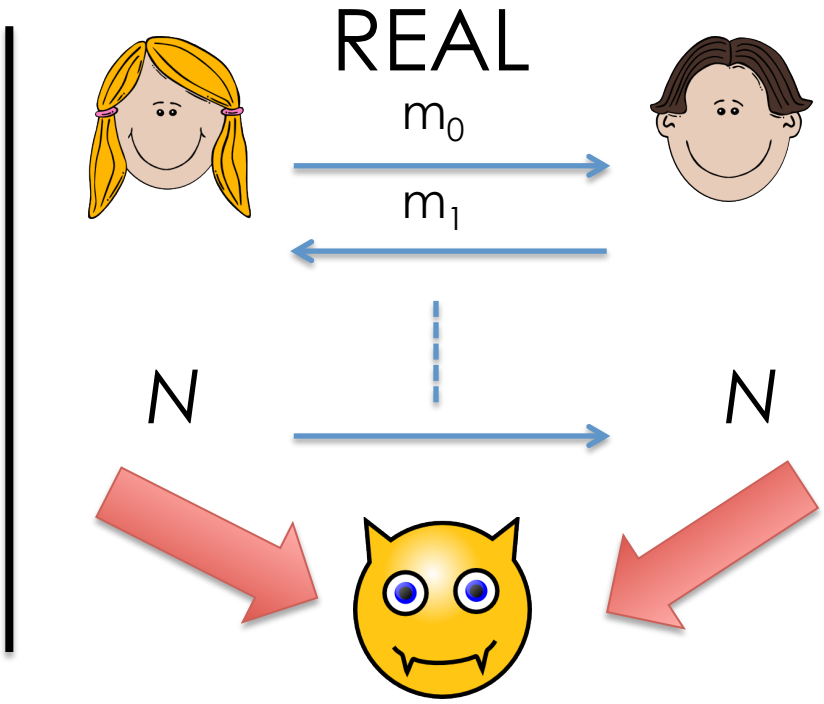
Example



- Securely computing RSA moduli

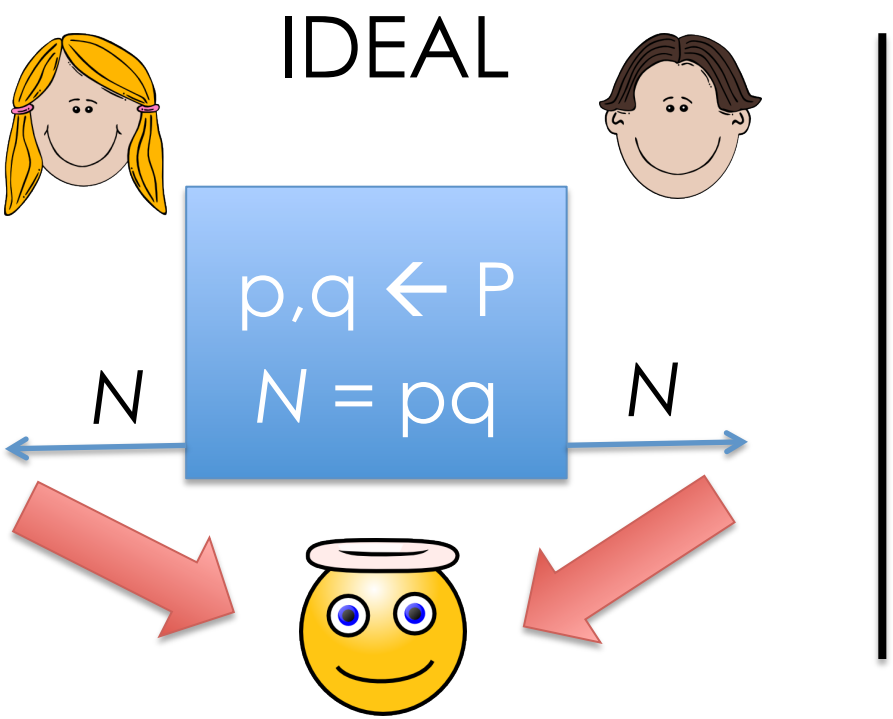
Example

Consider an Adv. that corrupts both parties at the end of the protocol



The Adversary outputs N and the parties random tapes

Example



The Simulator only gets *N*!

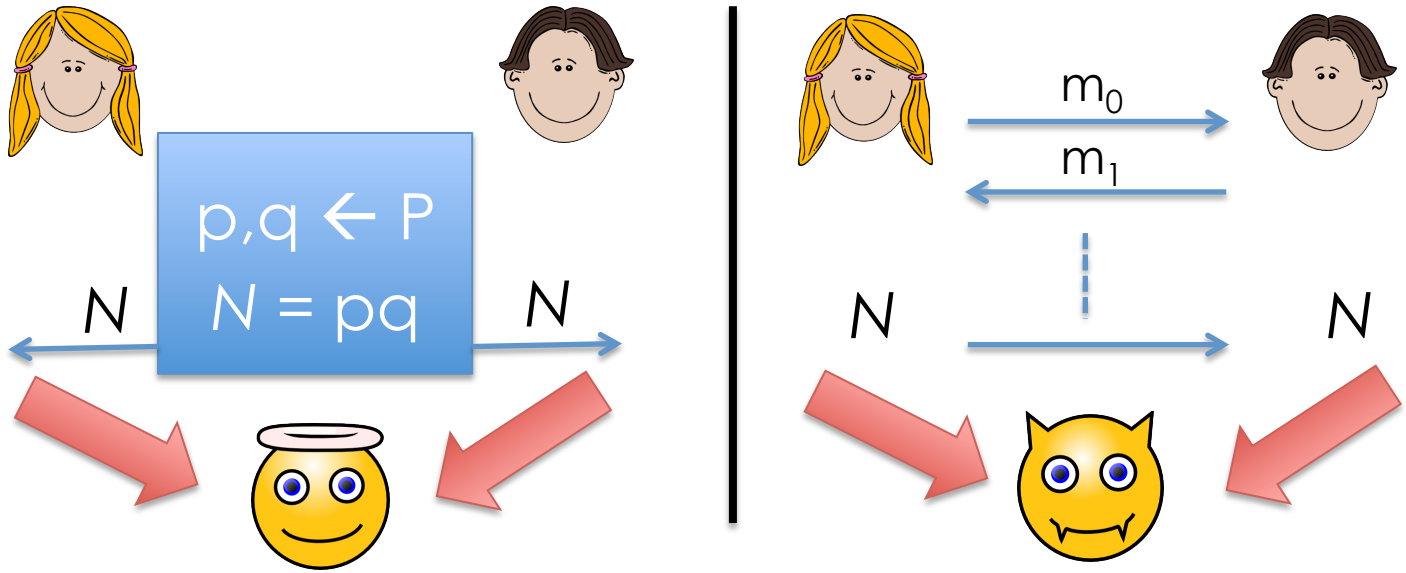
The Simulator needs to output random tapes for a run of the protocol that generates *N*

without knowing p and q!

Outline

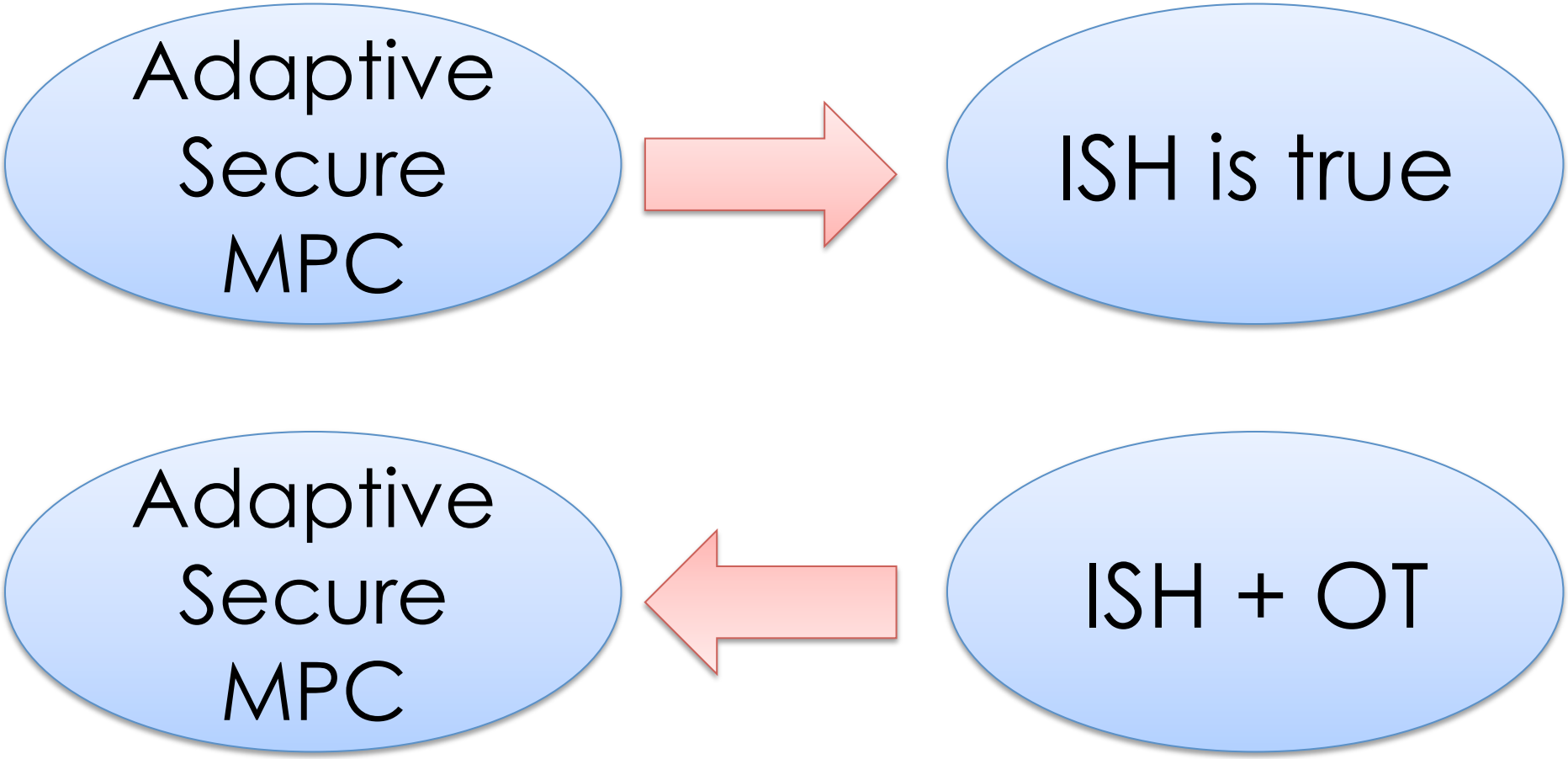
- Invertible Sampling Hypothesis (ISH)
- ISH is (conditionally) false
- ISH and Adaptive Secure MPC
- General AMPC is impossible

AMPC implies ISH

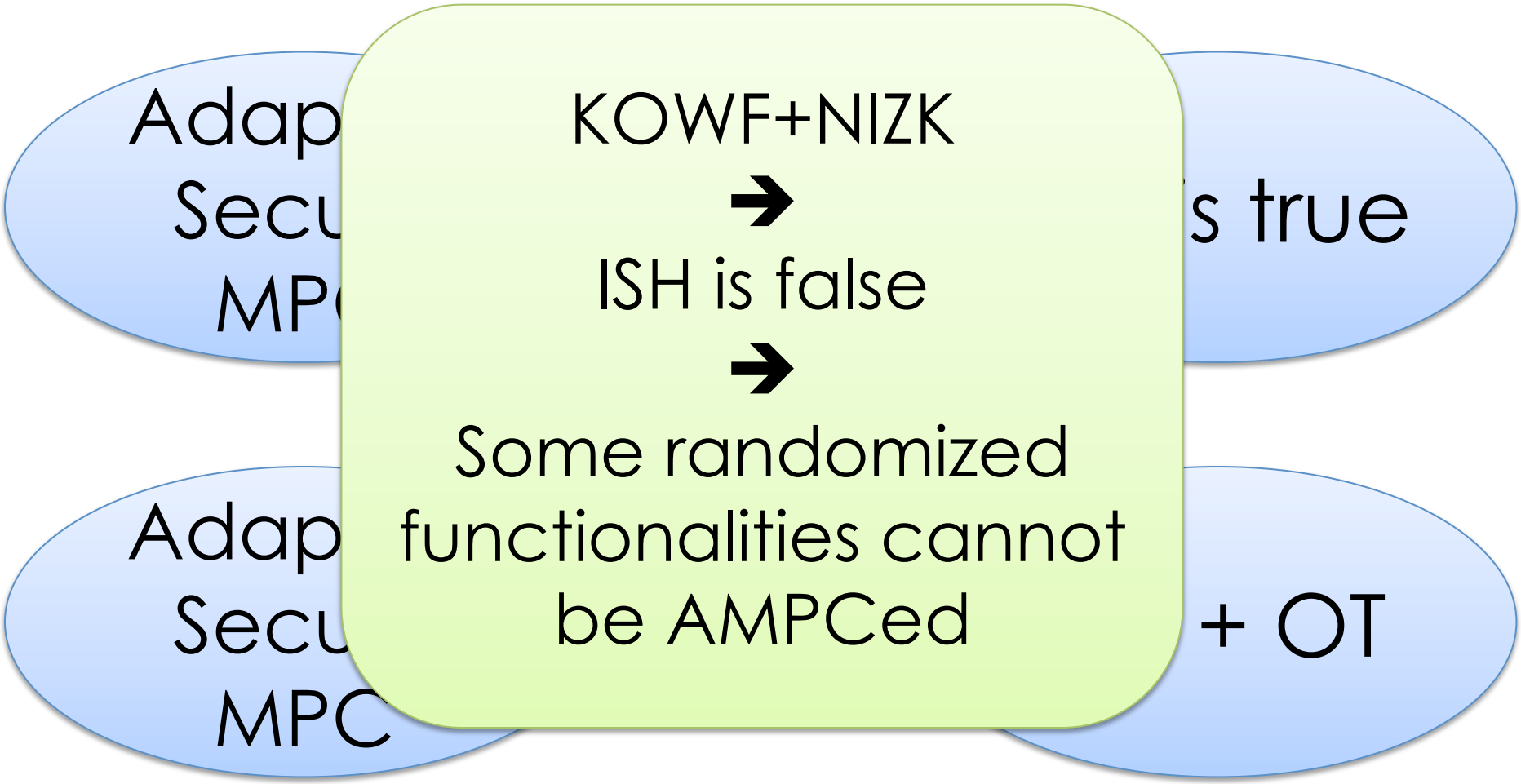


- Ideal functionality - **"Almost A"**
  - an algorithm that outputs RSA moduli
- Protocol and simulator - **"Almost B, B^{-1}"**
  - an alternative way of sampling (comp. close) RSA moduli in an invertible way.

ISH and Adaptive MPC



ISH and Adaptive MPC



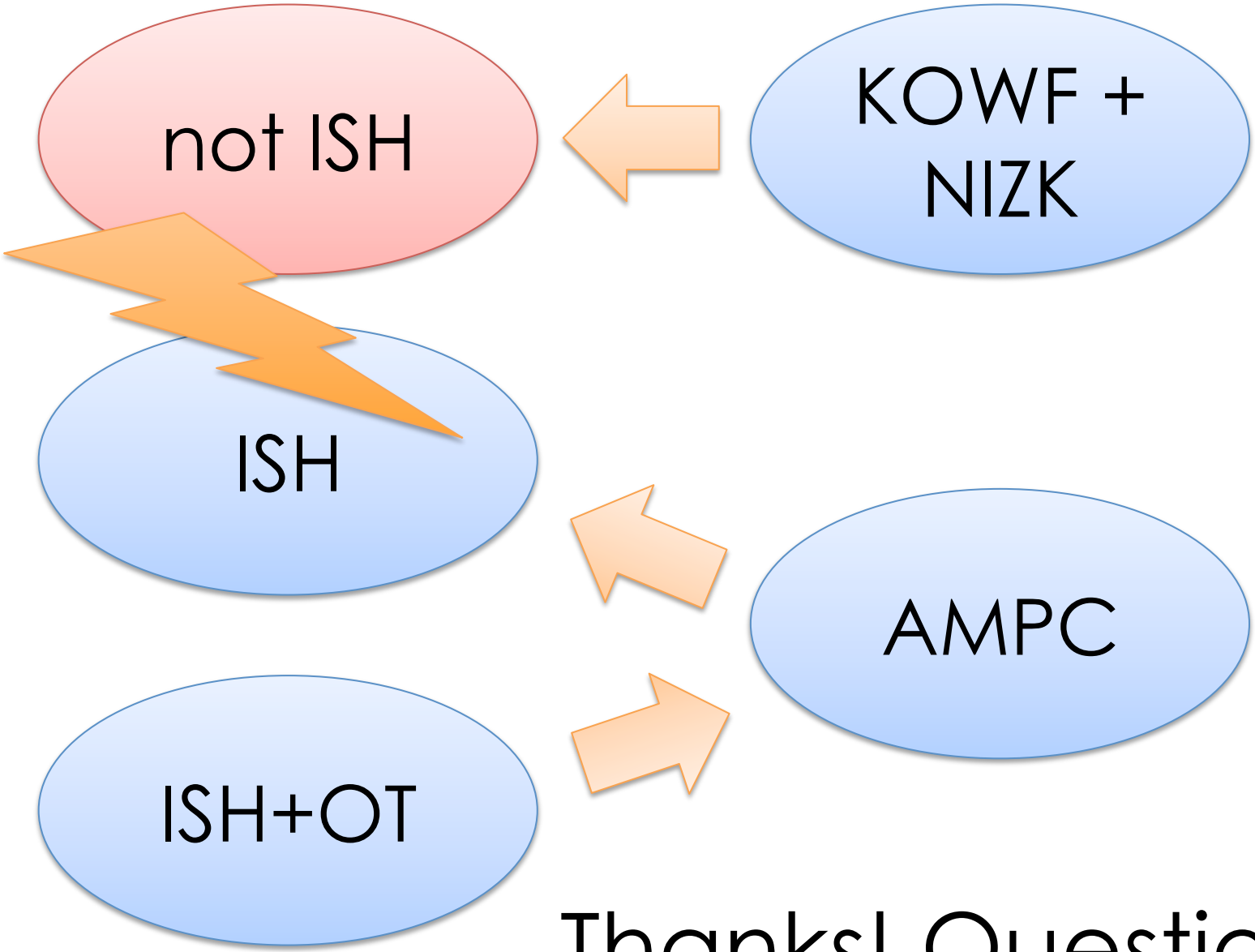
Open problems

Make result stronger

- Disprove ISH/AMPC with weaker assumptions

Invertible sampling for RSA?

- Find an algorithm that samples a distribution:
  - Computationally close to RSA moduli
  - In an invertible way



Thanks! Questions?