On Invertible Sampling and Adaptive Security

Yuval Ishai

Abishek Kumarasubramanian

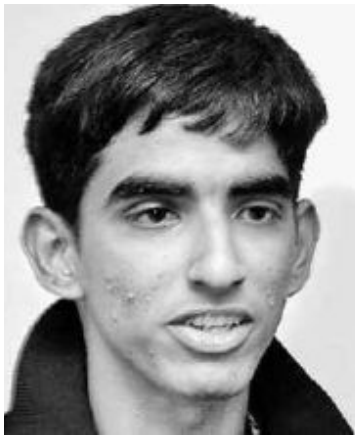
Claudio Orlandi

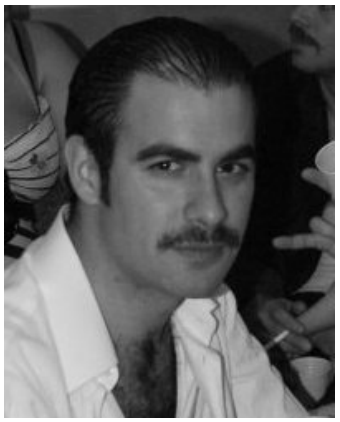
Amit Sahai

To appear at Asiacrypt 2010

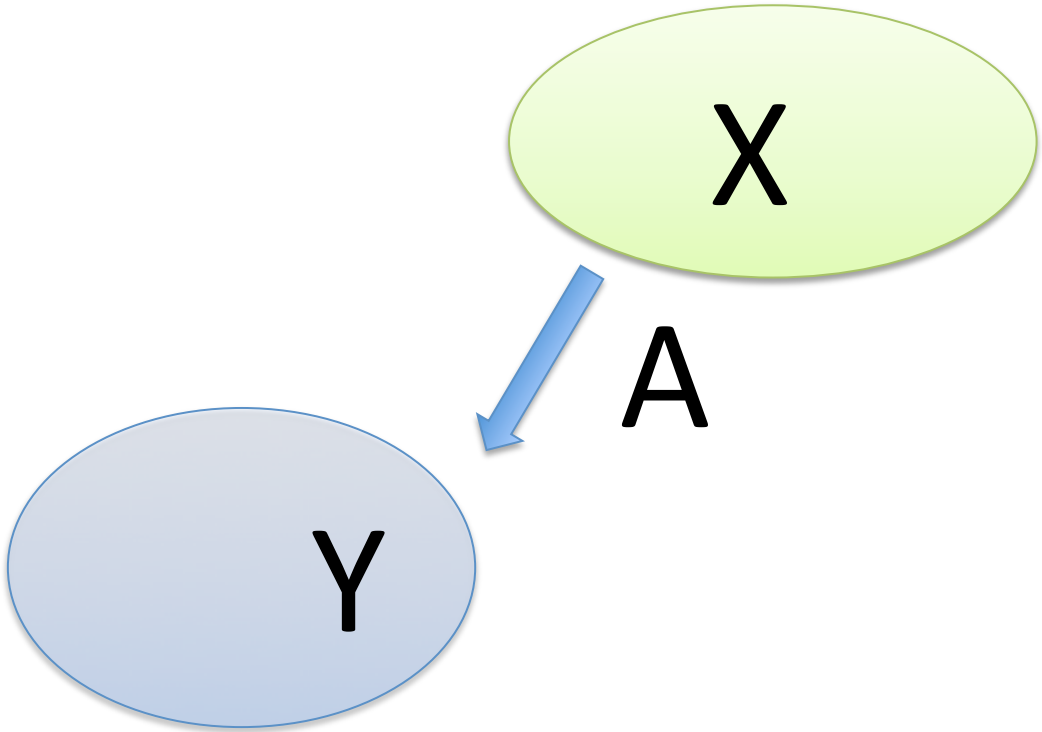
IKOS ‘04, ‘06, ‘07, ’08, ‘09

IKOS ‘10

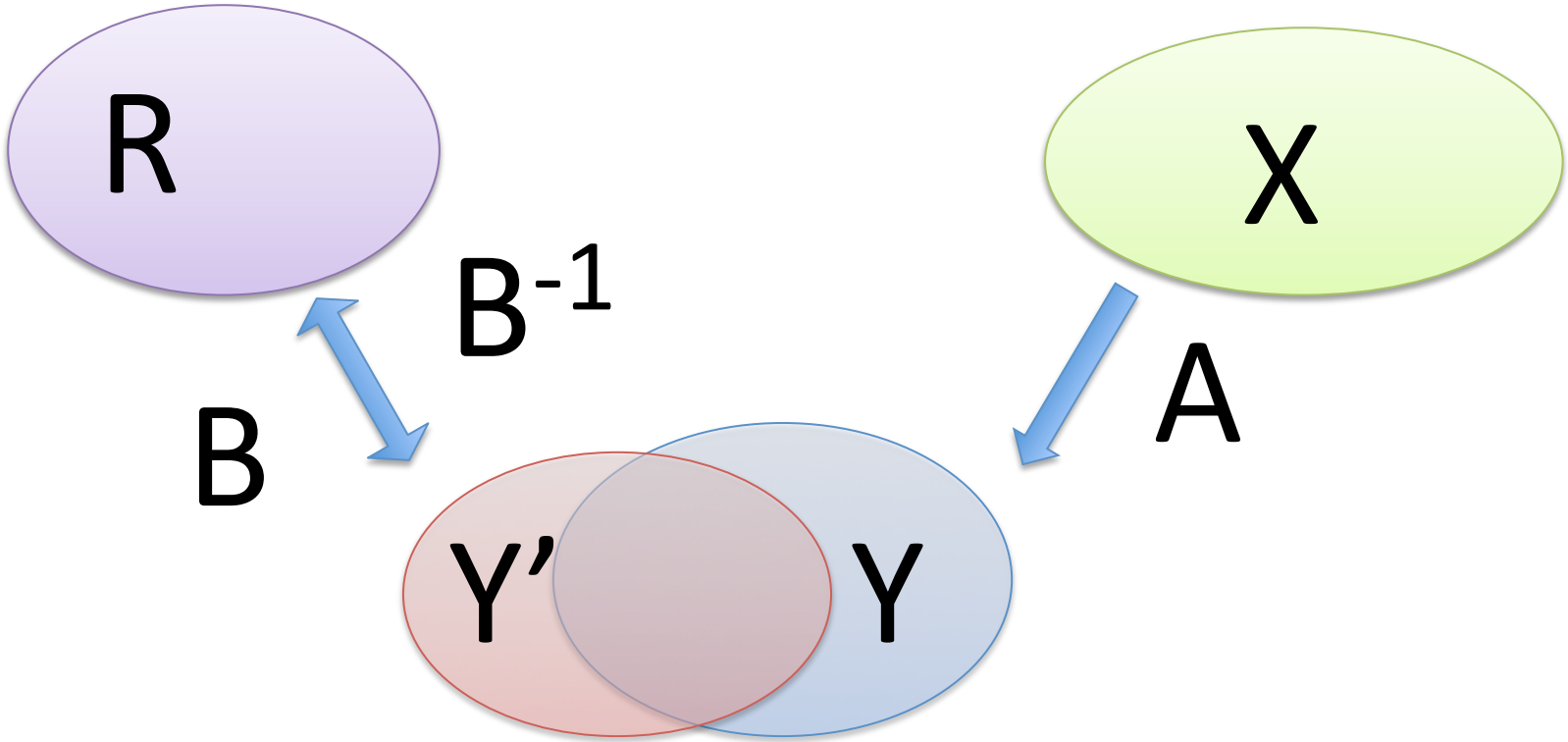




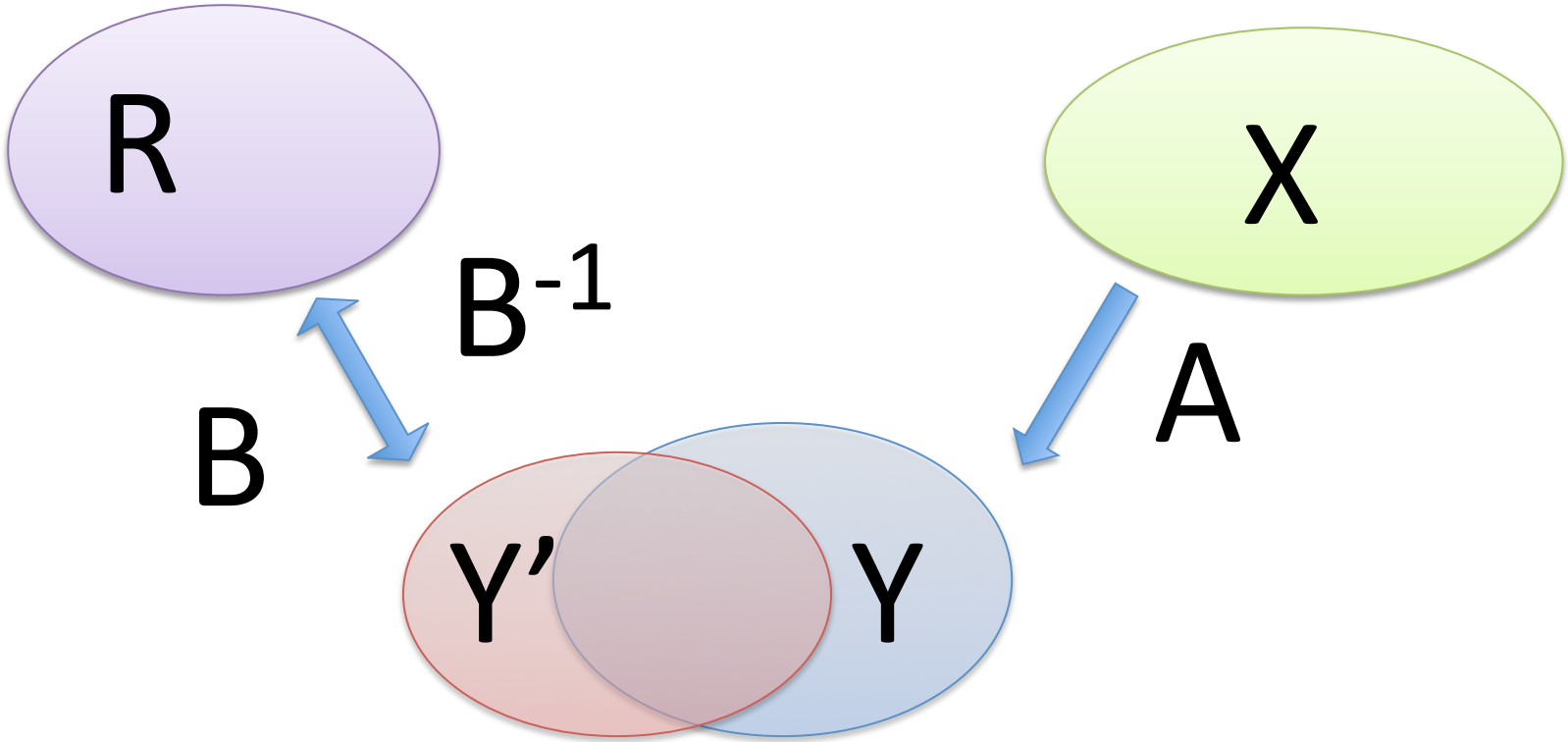
Invertible Sampling



Invertible Sampling

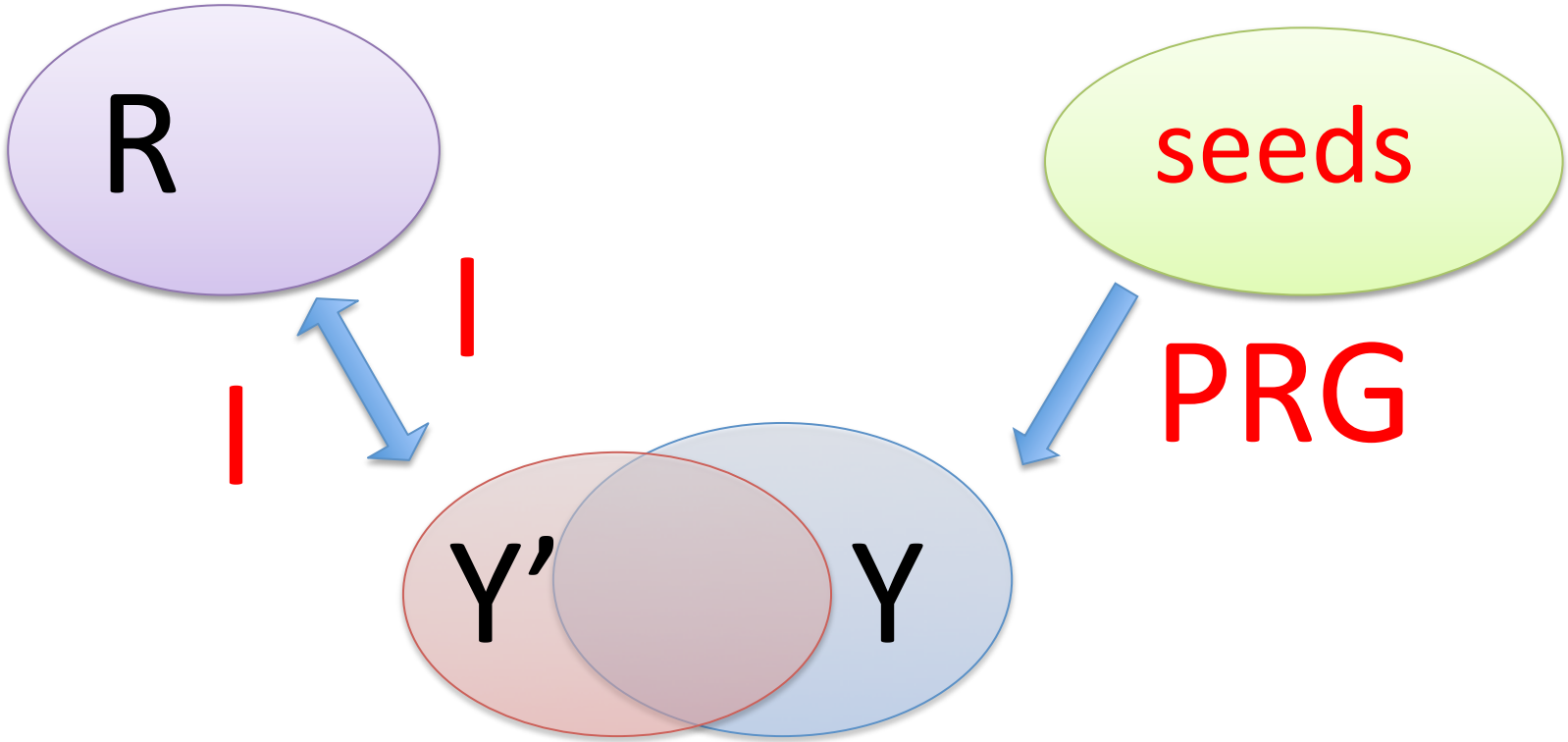


Invertible Sampling



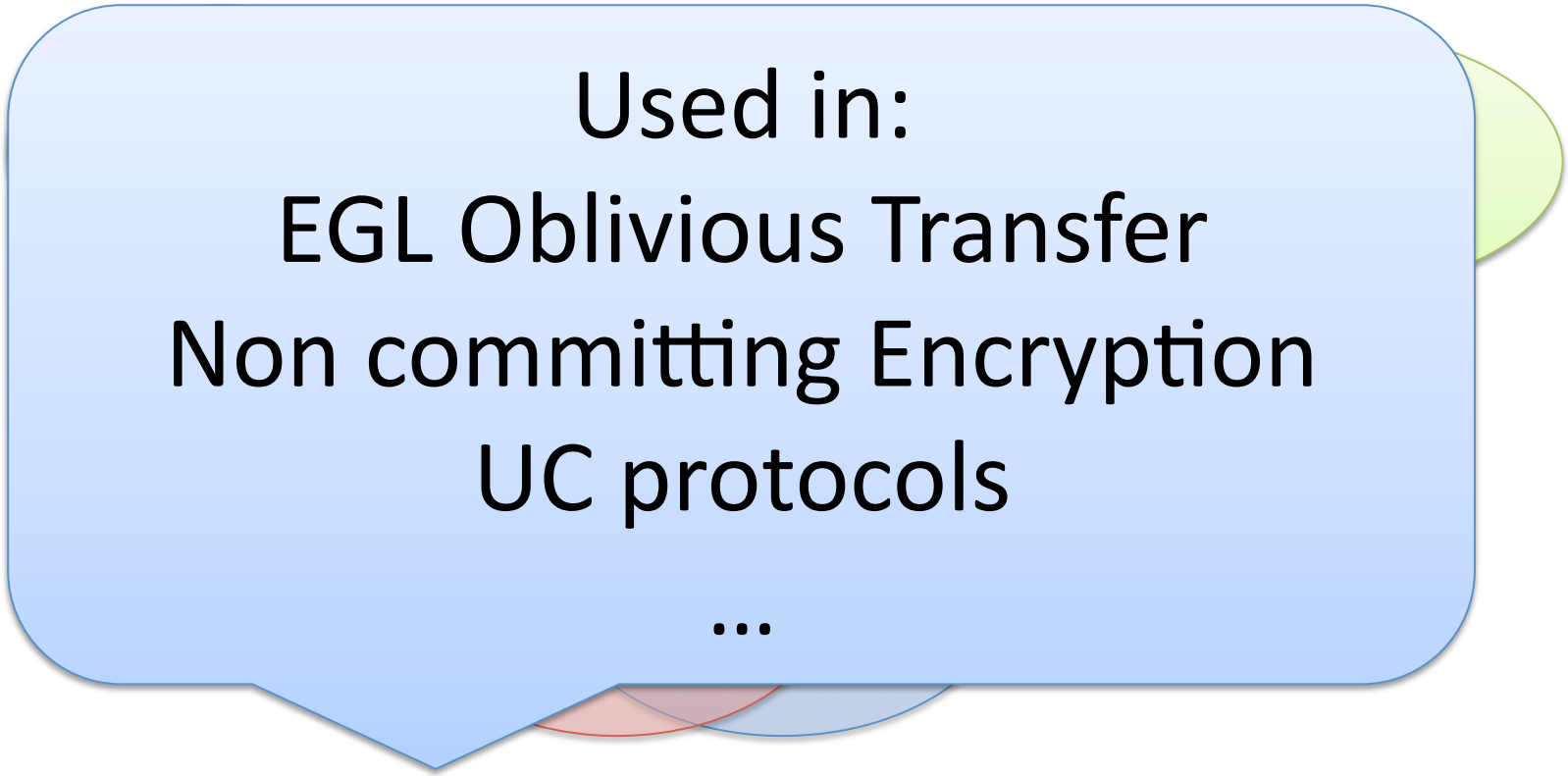
- 1) Y' and Y comp. ind.
- 2) B can be inverted – (even if A cannot)

Invertible Sampling



- 1) Y' and Y comp. ind.
- 2) B can be inverted – (even if A cannot)

Invertible Sampling



- 1) Y’ and Y comp. ind.
- 2) B can be inverted – (even if A cannot)

Inverse Sampling Hypothesis

Does every algorithm A satisfy 1) and 2) ?

Inverse Sampling Hypothesis

Does every algorithm A satisfy 1) and 2) ?

If KOWF + NIZK exist

➔ NO

Inverse Sampling Hypothesis

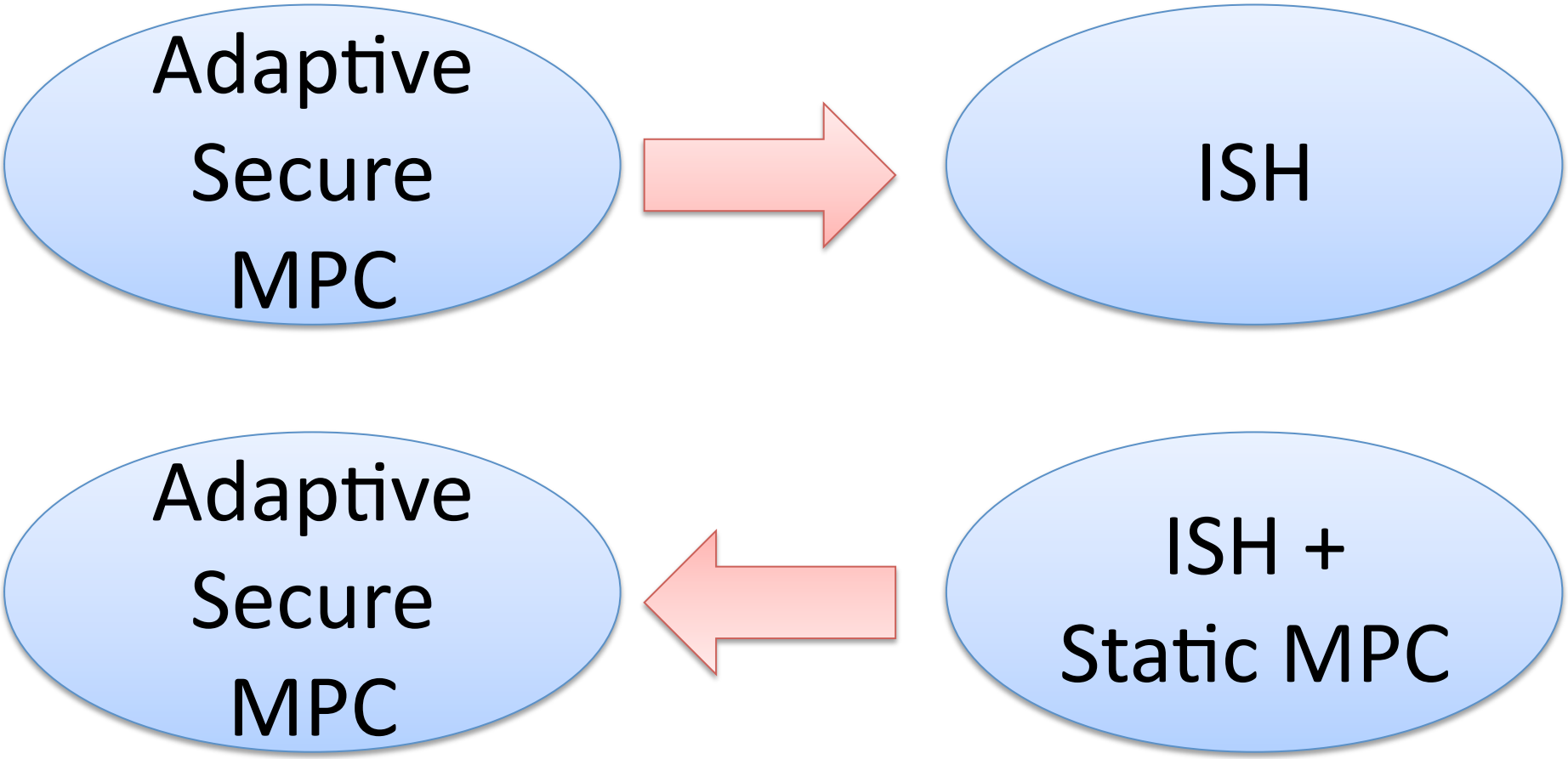
Does every algorithm A satisfy 1) and 2) ?

Canetti, Dakdouk '08 '09

If KOWF + NIZK exist

➔ NO

ISH and Adaptive MPC



ISH and Adaptive MPC