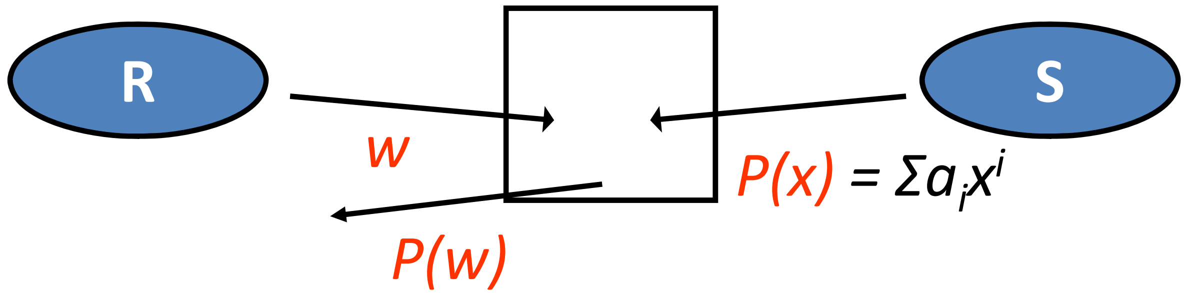
Some Consequences about Oblivious Polynomial Evaluation from Existence of the Homomorphic and Non-Committing Encryption

◎Chunhua Su*, Tadashi Araragi[$], Takashi Nishide *, Kouichi Sakurai*

*Department of Computer Science and Communication Engineering, Kyushu University

[$]NTT Communication Science Laboratories,
Nippon Telegraph and Telephone corporation.

1. OPE from Homomorphic Encryption

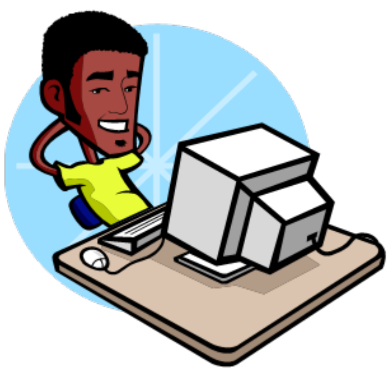


An efficient example of OPE:

The Receiver

$$Enc(w), Enc(w^2), ..., Enc(w^m)$$

The Sender



$$Enc(\sum_{i=0}^{m} a_i w^i) = Enc(P(w))$$

The receiver finally get the $P(w)$

Generate the keys of homomorphic encryption and the value *w*

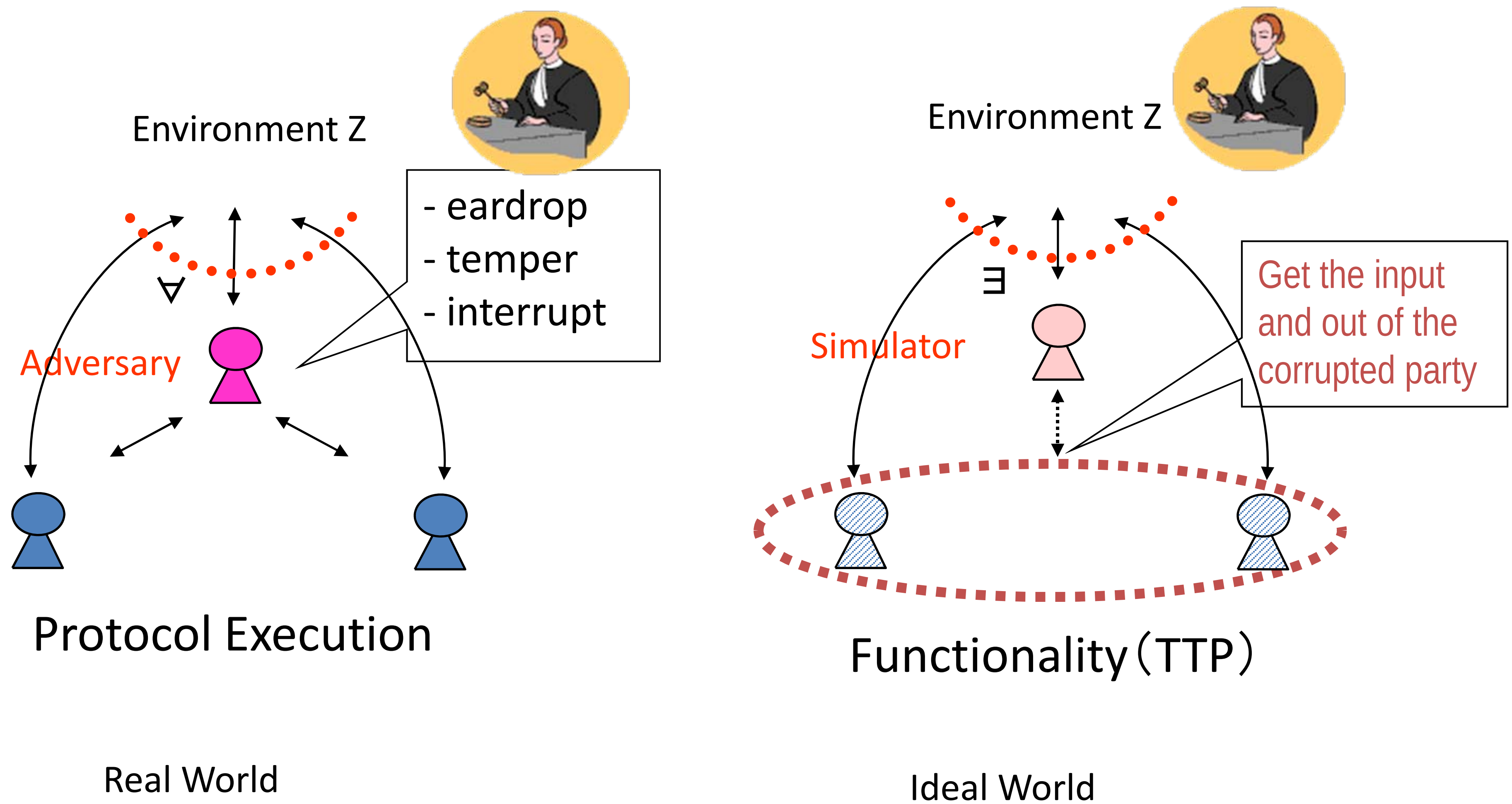
Generate a polynomial $P(x) = \sum_{i=0}^{m} a_i x^i$

Our goal: UC secure against malicious and adaptive adversary

The Problem: How to simulate the adaptive corruption?

2. Universal Composability and Adaptive Corruption

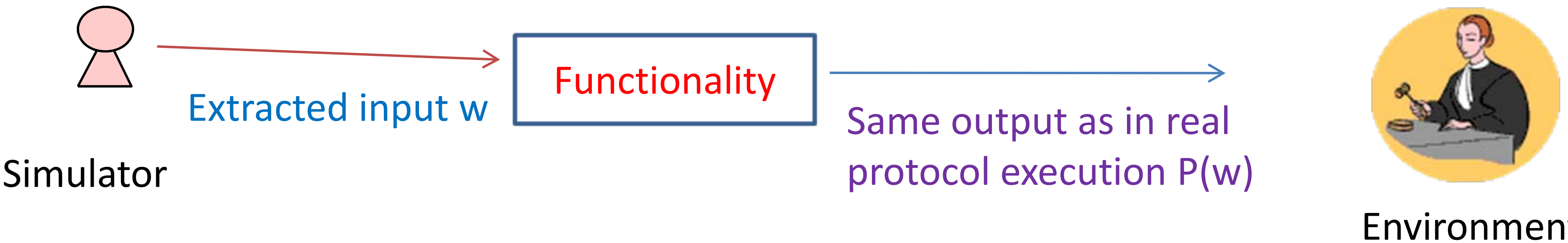
1. The environment can not distinguish the outputs from real world and ideal world.
2. Adaptive corruption: occur at any stage during the protocol execution.



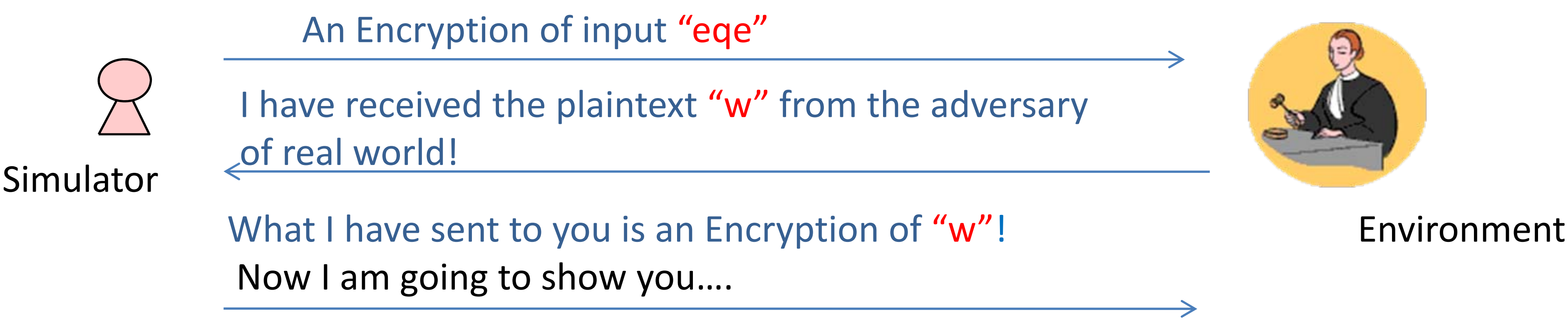
An Open Problem

Three conditions must be satisfied for an adaptively and UC secure OPE :

(1)Simulation Extractability: the simulator can extract the contents of any valid commitment/encryption generated by the adversary.



(2) Equivocality: simulator can generate some ”fake” ciphertexts that can later be explained as encryptions of anything.



Cont'd

(3) Homomorhpic Encryption:

$E(a; r_1)\ E(b; r_2)=E(a+b; R_1+R_2)$

- ◆Non-committing encryption is a good candidate which can satisfies condition (1) and (2), but does not satisfy (3).
- ◆Can we find a non-committing encryption with homomorphism?

A hint?

- Boneh et al. [BBS04]'s encryption scheme based on Decisional Linear DH Assumption:
- Public key: f, h, g ; Secret key: x, y so $f = g^x$, $h = g^y$
- Encrypt message m: $(u, v, w) = (f^r, h^s, g^{r+s}m)$
- Decrypt (u,v,w): $m = w\, u^{-1/x}\, v^{-1/y}$

Easy to get the equivocality and homomorphism with some modification, but diffcult to get the extractability

[BBS04] D. Boneh, X. Boyen, and H. Shacham. "Short group signatures". CRYPTO04, volume 3152 of LNCS, pp. 41–55. Springer, 2004.