Computational Hardness of Optimal Fair Computation: Beyond Minicrypt

Hemanta K. Maji Mingyuan Wang

PURDUE UNIVERSITY

August, 2021 (CRYPTO–2021)

Fair Coin-tossing

Coin-tossing Protocol

- Parties exchange a total of r messages.
- Parties agree on the output $b \in \{0, 1\}$ when the protocol ends.

Fair Coin-tossing

Fair coin-tossing: guaranteed output delivery

- A malicious party may pre-maturely abort.
- Honest party should still output a defense bit $b \in \{0, 1\}$.

Unfairness

ε-unfair: malicious party can deviate the expected output of the honest party by (at most) ε.

State-of-the-art: Impagliazzo's Five Worlds

	Secure Construction	Adversarial Attack
Pessiland	Fail-stop Adversary: $1/\sqrt{r}$-unfair	In General: Papadimitriou FOCS'83 constant-unfair Haitner Omri FOCS'11
		Fail-stop Adversary: $1/\sqrt{r}$-unfair Cleve Impagliazzo 93
Minicrypt	One-way Functions: $1/\sqrt{r}$-unfair Blum 82, Broder Dolev FOCS'84, Awerbuch Blum Chor Goldwasser Micali 85, Cleve STOC'86	$1/\sqrt{r}$-unfair Maji Wang CRYPTO'20
Cryptomania	Public-key Encryption:	$1/r$-unfair Cleve STOC'86
	Oblivious Transfer: $1/r$-unfair Moran Naor Segev TCC'09	

Optimal Fair Coin-tossing

$1/r$-unfair coin-tossing protocol is optimal.

State-of-the-art: Impagliazzo's Five Worlds

	Secure Construction	Adversarial Attack
Pessiland		In General: Papadimitriou FOCS'83 constant-unfair Haitner Omri FOCS'11
	Fail-stop Adversary: $1/\sqrt{r}$-unfair	Fail-stop Adversary: $1/\sqrt{r}$-unfair Cleve Impagliazzo 93
Minicrypt	One-way Functions: $1/\sqrt{r}$-unfair Blum 82, Broder Dolev FOCS'84, Awerbuch Blum Chor Goldwasser Micali 85, Cleve STOC'86	$1/\sqrt{r}$-unfair Maji Wang CRYPTO'20
Cryptomania	Public-key Encryption:	$1/r$-unfair Cleve STOC'86
	Oblivious Transfer: $1/r$-unfair Moran Naor Segev TCC'09	

Question

1. Is oblivious transfer necessary for optimal fair coin-tossing?
2. Are there fair coin-tossing with intermediate unfairness (e.g., $1/r^{3/4}$)?

Our results

	Secure Construction	Adversarial Attack
Pessiland		In General: Papadimitriou FOCS'83 constant-unfair Haitner Omri FOCS'11
	Fail-stop Adversary: $1/\sqrt{r}$-unfair	Fail-stop Adversary: $1/\sqrt{r}$-unfair Cleve Impagliazzo 93
Minicrypt	One-way Functions: $1/\sqrt{r}$-unfair Blum 82, Broder Dolev FOCS'84, Awerbuch Blum Chor Goldwasser Micali 85, Cleve STOC'86	$1/\sqrt{r}$-unfair Maji Wang CRYPTO'20
Cryptomania	Public-key Encryption:	$1/\sqrt{r}$-unfair This work
	PKE + f-hybrid, $f \not\to$ OT:	$1/\sqrt{r}$-unfair This work
	Oblivious Transfer: $1/r$-unfair Moran Naor Segev TCC'09	$1/r$-unfair Cleve STOC'86

f-hybrid, where $f \not\to$ OT

- Parties have access to a trusted party realizing (possibly randomized) f.
- Could potentially be useful (e.g., UC-secure commitments Maji Prabhakaran Rosulek CRYPTO'10, realizing other functionalities Rosulek Shirley TCC'18)

Open problem

What we did not prove

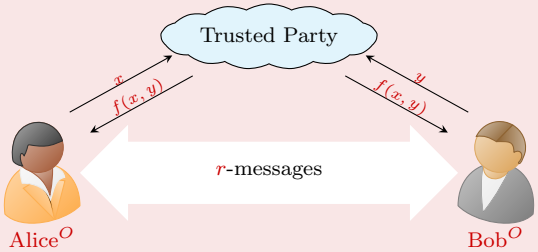
- We did not present a set of oracles relative to which
  1. A secure protocol for f exists;
  2. optimal fair coin-tossing protocol does not exist.
- That is, we did not prove a black-box separation between "securely realizing f" and "optimal fair coin-tossing"
  - We only give parties access to a trusted party realizing f
  - Parties could use the "oracles implementing f" in ways other than merely evaluating f
- Proving a black-box separation result would imply a separation between
  1. securely realizing (incomplete) f
  2. oblivious transfer

Relevant works

- Haitner Makriyannis Omri TCC'18 proved that
  - There exists a universal constant c, such that for any constant r, the existence of r-message coin-tossing protocol with unfairness $< c/\sqrt{r}$ implies the existence of (infinitely-often) key agreement protocols.
- Incomparable to ours: proves a stronger consequence but for constant-round protocols.

Our results

Our model



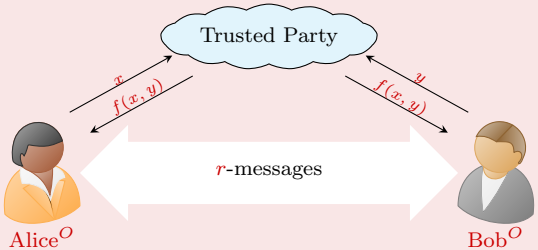
- A set of oracles O facilitating public-key encryption.
- A trusted party realizing f (unfairly)
  - Adversary receives the output $f(x,y)$ first. May abort and block the output delivery to the honest party.

Given fair f, fair coin-tossing with 0-unfairness is possible

Suppose $f = \mathsf{XOR}$. Alice samples her input $x \in \{0,1\}$ uniformly at random. Bob samples his input $y \in \{0,1\}$ uniformly at random. Output $f(x,y)$ as the output of the protocol. This protocol is completely fair.

Our results

Our model



Our results

There exists a fail-stop adversary who could deviate the expected output of the honest party by $\Theta(1/\sqrt{r})$. This adversary asks (at most) polynomially additionally queries to O.

Proof Overview

Attacker of Maji Wang CRYPTO'20

Present a fail-stop attacker that deviates the expected output by $1/\sqrt{r}$ for any fair coin-tossing in the random oracle model.

- We note that their attacker generalizes to other settings as long as the following invariant is maintained.

Invariant

Alice and Bob private views are (close to) independent conditioned on the partial transcript.

- For the random oracle model, they use the "heavy querier" (Impagliazzo Rudich STOC'89, Barak Mahmoody CRYPTO'09) to ensure this invariant.

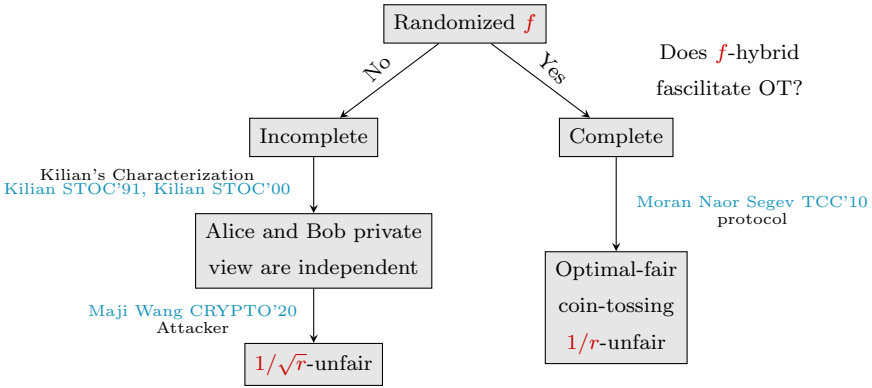
Separation from PKE

Mahmoody Maji Prabhakaran TCC'14

- Define a set of oracles O that facilitates PKE.
- For any two-party interactive protocol where Alice and Bob have access to O, there is a "*common information learner*" that asks polynomially queries to ensure that Alice and Bob private views are (close to) independent.

Any coin-tossing protocol that uses public-key encryption in a black-box manner is $1/\sqrt{r}$-unfair.

A Dichotomy for f-hybrid



- There might be a t-round secure protocol for f. Simply replacing f-hybrid with the t-round protocol is not sufficient to rule out optimal fair coin-tossing.
- There does not exist a secure protocol for f. f-hybrid could be useful for other tasks.

  Rosulek Shirley TCC'18

Thanks!

Full version eprint.iacr.org/2021/882