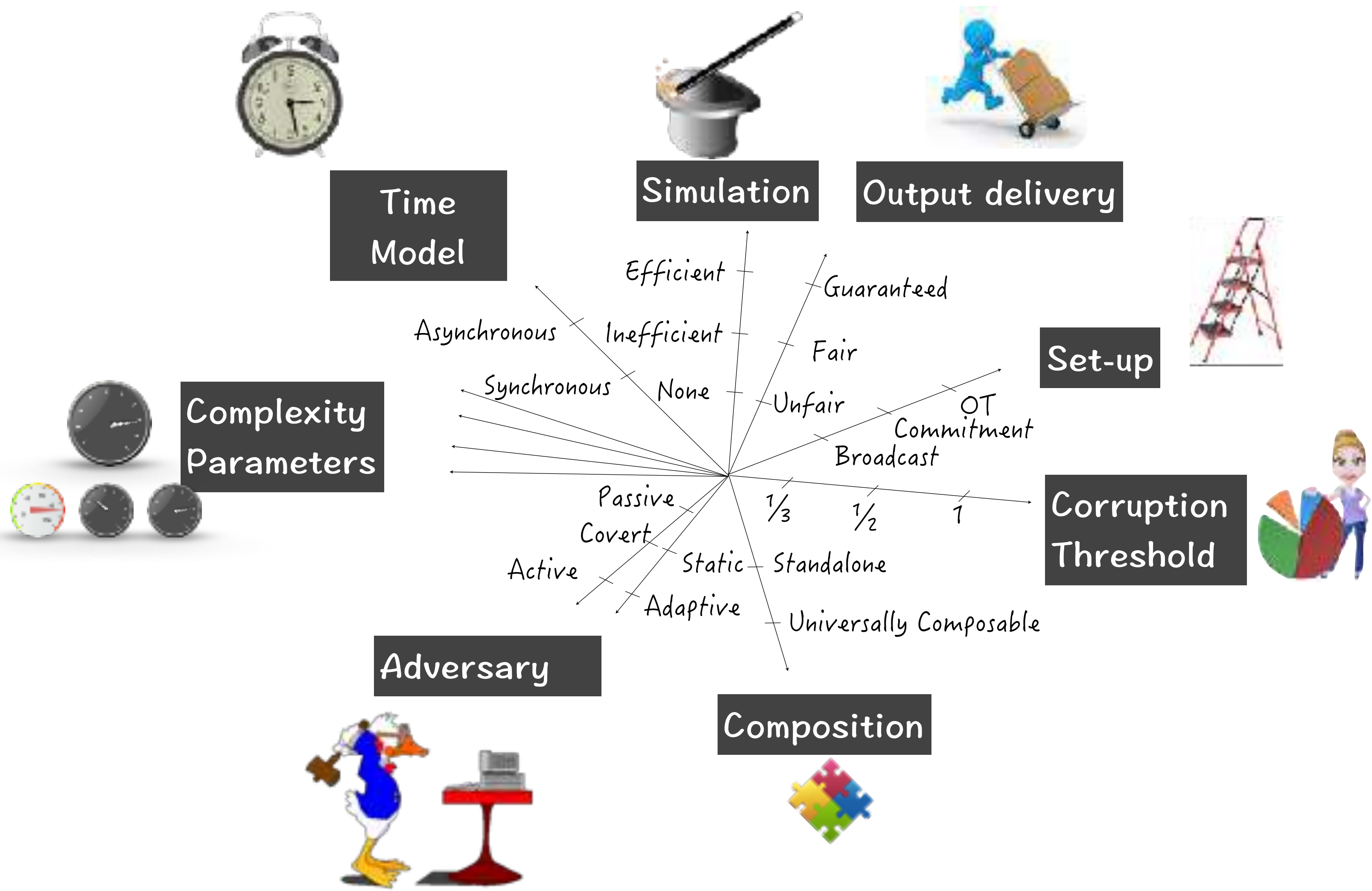
Advanced Tools from Modern Cryptography

Lecture 14

MPC: Feasibility Results Summary

MPC Dimensions



Basic Dimensions

- Adversary's computational power: PPT adversary, Information-theoretic security
- Honest majority: Thresholds 1 (no honest majority), ½ and ⅓
- Security Level: Passive security, UC security with selective abort, or UC security with guaranteed output delivery
- Setup: Point-to-point channels, Broadcast, Common Reference String (CRS), OT

General MPC

- Information-theoretic security
  - Passive with corruption threshold t < n/2 — Passive BGW/CCD
  - Passive with OT setup — Passive GMW
  - Guaranteed Output UC with t < n/3 — BGW
  - Guaranteed Output UC with t < n/2 and Broadcast — "Rabin-BenOr"
  - Selective Abort UC, with OT — "Kilian." (Also: GMW paradigm implemented using OT-based proof)
- Computational security
  - Passive — Composing Yao or Passive GMW with a passive-secure OT protocol
  - Standalone — GMW: using ZK proofs
  - Selective Abort UC, with CRS — Composing Kilian with a CRS-based UC-secure OT protocol

Beyond General MPC

- In each model, only some functionalities will be realisable without setups (will call them **trivial** functionalities)
  - Question: which functions are trivial in each model?

Trivial Functionalities: Passive Information-Theoretic

- For n-party information-theoretic passive security, which functions for each corruption threshold t
- Called the **Privacy Hierarchy**
  - All n-party functions appear at level $\lfloor (n-1)/2 \rfloor$ in this hierarchy (e.g., by Passive-BGW). Some are at level n: e.g., XOR or more generally, group addition. Level n-1 is same as level n.
  - At all intermediate levels t, examples known to exist which are not in level t+1
  - Open problem: characterise all functions at level t (or even at level n)
    - For n=2, we do have a characterisation for all t (t=0,2)

Trivial 2-Party Functionalities: Information-Theoretic

- Passive security. (Restricting to symmetric SFE.)
  - Deterministic SFE: Trivial $\Leftrightarrow$ Decomposable

Decomposable Function

Decomposable

	1	3
0	1	3
2	2	3

“Max”
(no ties)

	0	1
0	0	1
1	1	0

XOR

	1	2	3
0	1	1	2
1	3	4	4

$\lceil (x+5y)/2 \rceil$

1	1	2	2
3	4	4	3

Undecomposable

	0	1
0	0	0
1	0	1

1	1	2
4	5	2
4	3	3

“Spiral”

1	1	4	2
4	3	3	2
4	2	1	1

Trivial 2-Party Functionalities: Information-Theoretic

- Passive security. (Restricting to symmetric SFE.
  - Deterministic SFE: Trivial ⇔ Decomposable
  - Open for randomized SFE!
- Standalone security
  - Deterministic SFE:
    Trivial ⇔ Uniquely Decomposable and Saturated

Decomposable Function

Decomposable

	1	3
0	1	3
2	2	3

	0	1
0	0	1
1	1	0

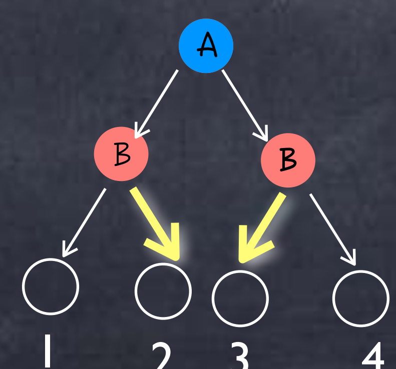
1	1	2
3	4	4

1	1	2	2
3	4	4	3

Not Uniquely Decomposable

Not Saturated

This strategy doesn't correspond to an input



Trivial 2-Party Functionalities: Information-Theoretic

- Passive security. (Restricting to symmetric SFE.
  - Deterministic SFE: Trivial ⇔ Decomposable
  - Open for randomized SFE!
- Standalone security
  - Deterministic SFE:
    Trivial ⇔ Uniquely Decomposable and Saturated
- UC security
  - Trivial ⇔ Splittable

Trivial Functionalities: PPT Setting

- Under the assumption that there is a passive-secure protocol for OT (a.k.a. sh-OT)
  - For passive & standalone security: all n-party functionalities are trivial
  - For UC security: very few are trivial irrespective of computational hardness
    - Recall, for n=2: UC trivial ⇔ Splittable. Gives explicit characterisation (e.g., functions like f(x,y)=x)
    - Full characterisation open for $n \geq 3$

Completeness

- We saw OT can be used to (passive- or UC-) securely realise any functionality
  - i.e., any other functionality can be reduced to OT
- The Cryptographic Complexity question:
  - Can F be reduced to G (for different reductions)?
  - F reduces to G: will write $F \sqsubseteq G$
  - G **complete** if everything reduces to G
  - F **trivial** if F reduces to everything (in particular, to NULL)

PPT Setting: Completeness

- PPT Passive security and PPT Standalone security
  - Under sh-OT assumption, all functions are trivial — and hence all are complete too!
- PPT UC security, n=2:
  - Recall, only a few (splittable) functionalities are trivial
  - Under sh-OT, turns out that every non-trivial functionality is complete

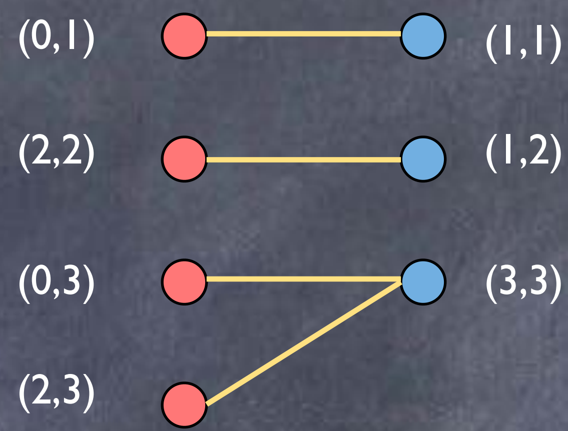
IT Setting: Completeness

- Information-Theoretic Passive security
  - (Randomized) SFE: Complete $\Leftrightarrow$ Not Simple
  - What is Simple?

Simple vs. Non-Simple

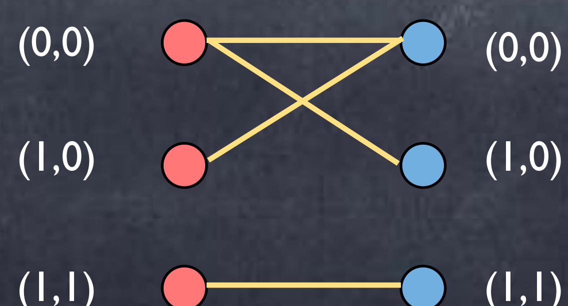
Edge ((x,a),(y,b)) exists iff f(x,y)=(a,b)

	1	3
0	1	3
2	2	3



Simple:
Each connected component is a biclique

	0	1
0	0	0
1	0	1

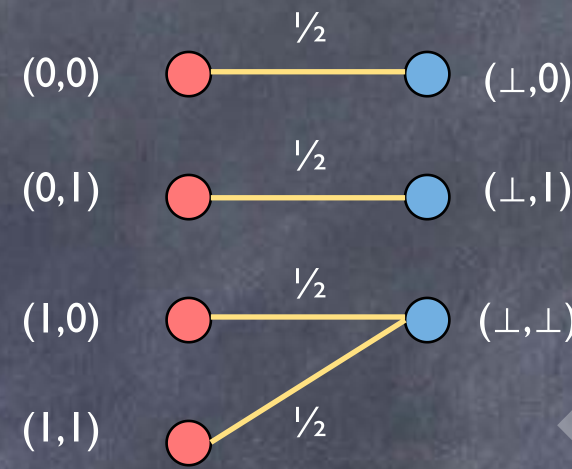


IT Setting: Completeness

- Information-Theoretic Passive security
  - (Randomized) SFE: Complete ⇔ Not Simple
  - What is Simple?
    - In the characteristic bipartite graph, each connected component is a biclique
      - If randomized, within each connected component $w(u,v) = w_A(u) \times w_B(v)$

Simple vs. Non-Simple (Randomized)

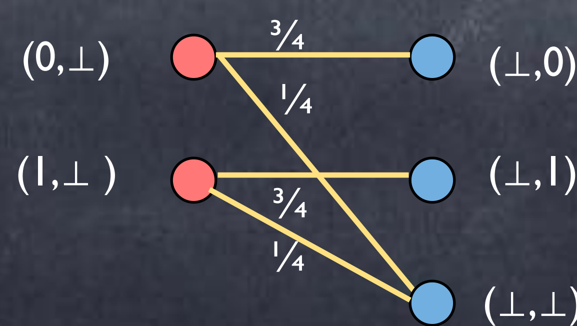
Optionally one-sided coin-toss



Edge ((x,a),(y,b)) weighted with Pr[(a,b) | (x,y)] where x,y inputs and a,b outputs

Simple: within connected component $w(u,v) = w_A(u) \cdot w_B(v)$

Rabin-OT



IT Setting: Completeness

- Information-Theoretic Passive security
  - (Randomized) SFE: Complete ⇔ Not Simple
- Information-Theoretic Standalone & UC security
  - (Randomized) SFE: Complete ⇔ Core is not Simple
  - What is the core of an SFE?
    - SFE obtained by removing "redundancies" in the input and output space

A Map of 2-Party Functions