Advanced Tools from Modern Cryptography

Lecture 15

MPC: Beyond General MPC

Recall

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

Feasibility of General MPC

- Given honest majority, or given OT as a setup:
  - General MPC is possible with the highest security guarantee (information-theoretic, UC security)
    - Variations: t<n/3 vs. t<n/2+broadcast. Perfect vs. Statistical. Guaranteed output delivery vs. unfair.
- Otherwise:

Otherwise:	Passive	Stand-alone	UC
PPT	✓	✓	✗
Info. Th.	✗	✗	✗

- When general MPC is not possible, which functions admit MPC?
  - A functionality that admits MPC protocols without a setup in a security model is called trivial in that model

Trivial Functionalities: PPT Setting

General MPC under the assumption that there is a passive-secure protocol for OT (a.k.a. sh-OT)

For n=2, we have an explicit characterisation of trivial functions (splittable functions). Extends to n=3 as well.

Open for n > 3

	Passive	Stand-alone	UC
PPT	✓	✓	✗
Info. Th.	✗	✗	✗

GMW: using ZK proofs (sh-OT ⇒ OWF ⇒ ZK)

Trivial Functionalities: Information-Theoretic

- For n-party information-theoretic passive security, for each corruption threshold t: the **Privacy Hierarchy**
  - All n-party functions appear till level $\lfloor (n-1)/2 \rfloor$ in this hierarchy (e.g., by Passive-BGW). Some reach 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: For all n, characterise the functions at each level t (or even for t=n)
    - For n=2 we do have a characterisation

Trivial 2-Party Functionalities: Information-Theoretic

	Passive	Stand-alone	UC
PPT	✓	✓	✗
Info. Th.	✗	✗	✗

For deterministic SFE:
Trivial ⇔ Decomposable

Decomposable Function

(For simplicity will restrict to symmetric SFE)

Examples of Decomposable Functions

	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

Examples of Undecomposable Functions

	0	1
0	0	0
1	0	1

AND

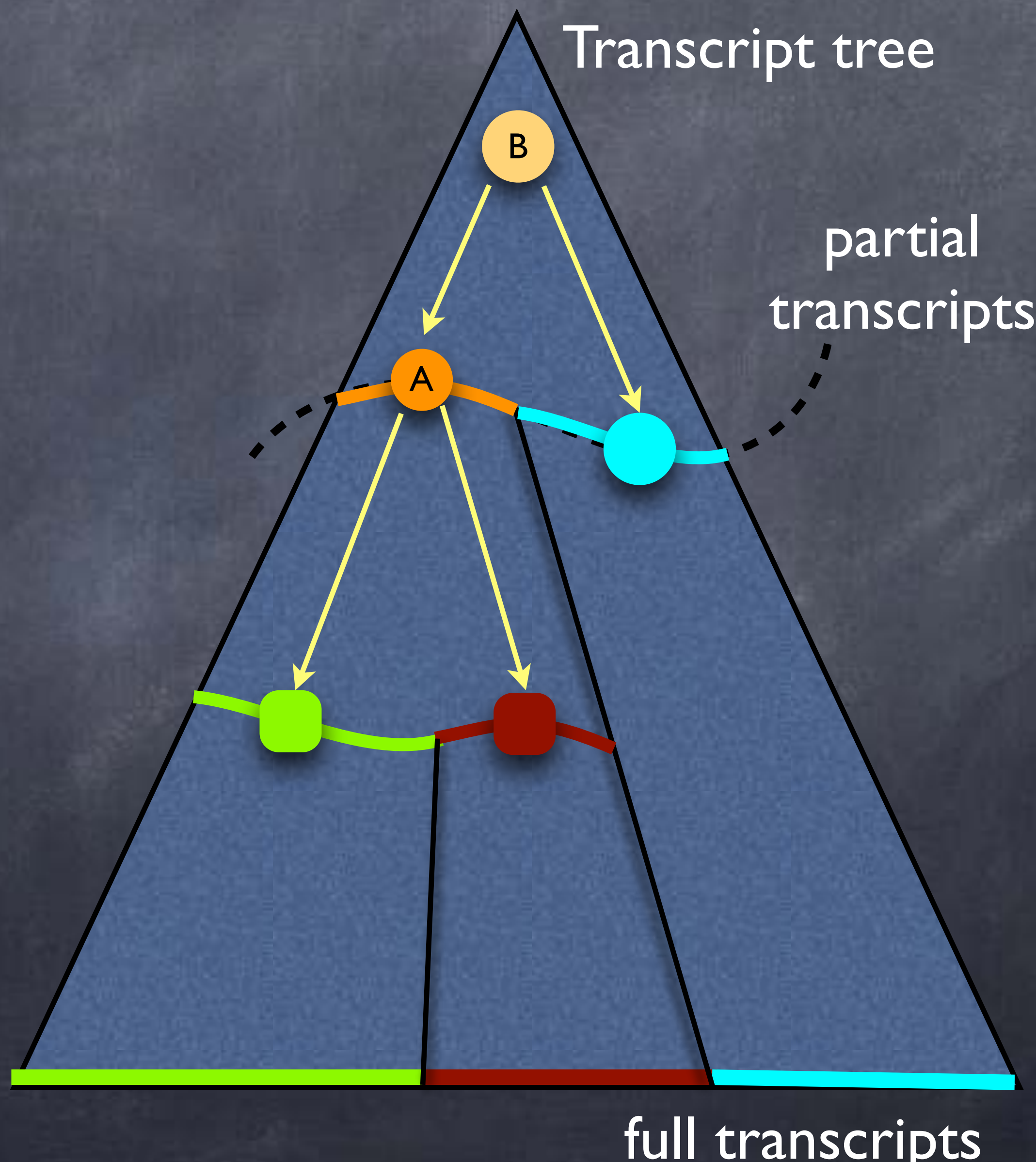
1	1	2
4	5	2
4	3	3

"Spiral"

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

Decomposable Function

	1	3
0	1	3
2	2	3



Trivial 2-Party Functionalities: Information-Theoretic

	Passive	Stand-alone	UC
PPT	✓	✓	✗
Info. Th.	✗	✗	✗

For deterministic SFE:
Trivial ⇔ Decomposable

Open for randomized

For deterministic SFE:
Trivial ⇔ Uniquely Decomposable & Saturated

Decomposable Function

Examples of Decomposable Functions

	1	3
0	1	3
2	2	3

	0	1
0	0	1
1	1	0

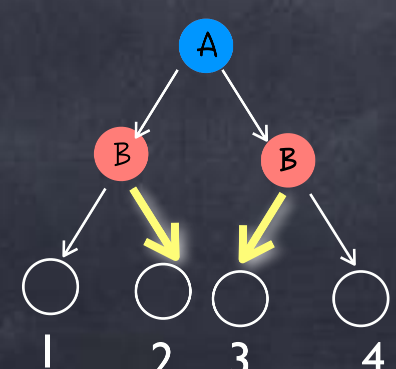
Not Uniquely Decomposable

1	1	2
3	4	4

Not Saturated

1	1	2	2
3	4	4	3

This strategy doesn't correspond to an input



Trivial 2-Party Functionalities: Information-Theoretic

Trivial ⇔ Splittable

	Passive	Stand-alone	UC
PPT	✓	✓	✗
Info. Th.	✗	✗	✗

For deterministic SFE:
Trivial ⇔ Decomposable

Open for randomized

For deterministic SFE:
Trivial ⇔ Uniquely Decomposable & Saturated

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

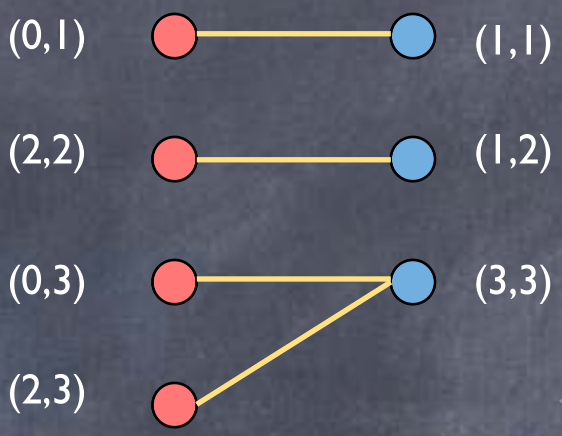
IT Setting: Completeness

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

Simple vs. Non-Simple

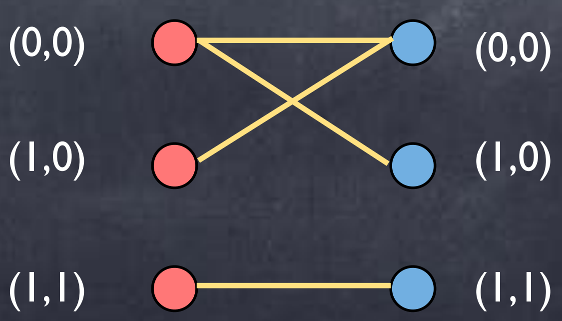
Edge ((x,a),(y,b)) exists iff f(x,y)=(a,b)

	1	3
0	1	3
2	2	3



Simple: Each connected component is a biclique

	0	1
0	0	0
1	0	1

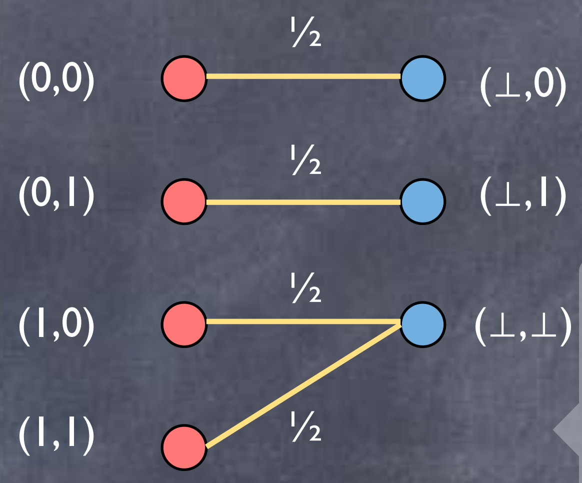


IT Setting: Completeness

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

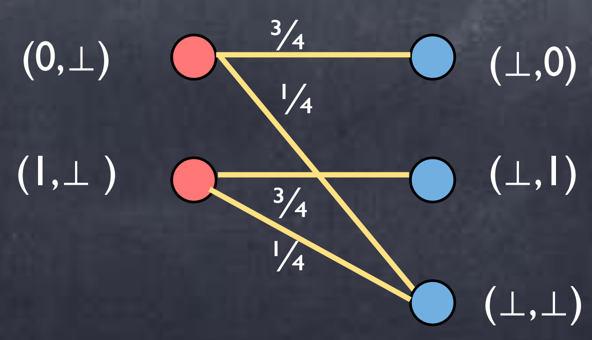
Simple vs. Non-Simple (Randomized)

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 $\Leftrightarrow$ Not Simple
- Information-Theoretic Standalone & UC security
  - (Randomized) SFE: Complete $\Leftrightarrow$ 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