AN ABSTRACTION FOR "GENERAL ASSUMPTIONS"

USING MPC FUNCTIONALITIES

MANOJ PRABHAKARAN

(BASED ON JOINT WORK WITH
HEMANTA MAJI & MIKE ROSULEK)

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

MPC FUNCTIONALITIES

MPC FUNCTIONALITIES

- Different MPC functionalities encapsulate different ways one can "access" information
  - Access to learning information and influencing information
  - e.g. OT, key exchange, coin-tossing, commitment, ...

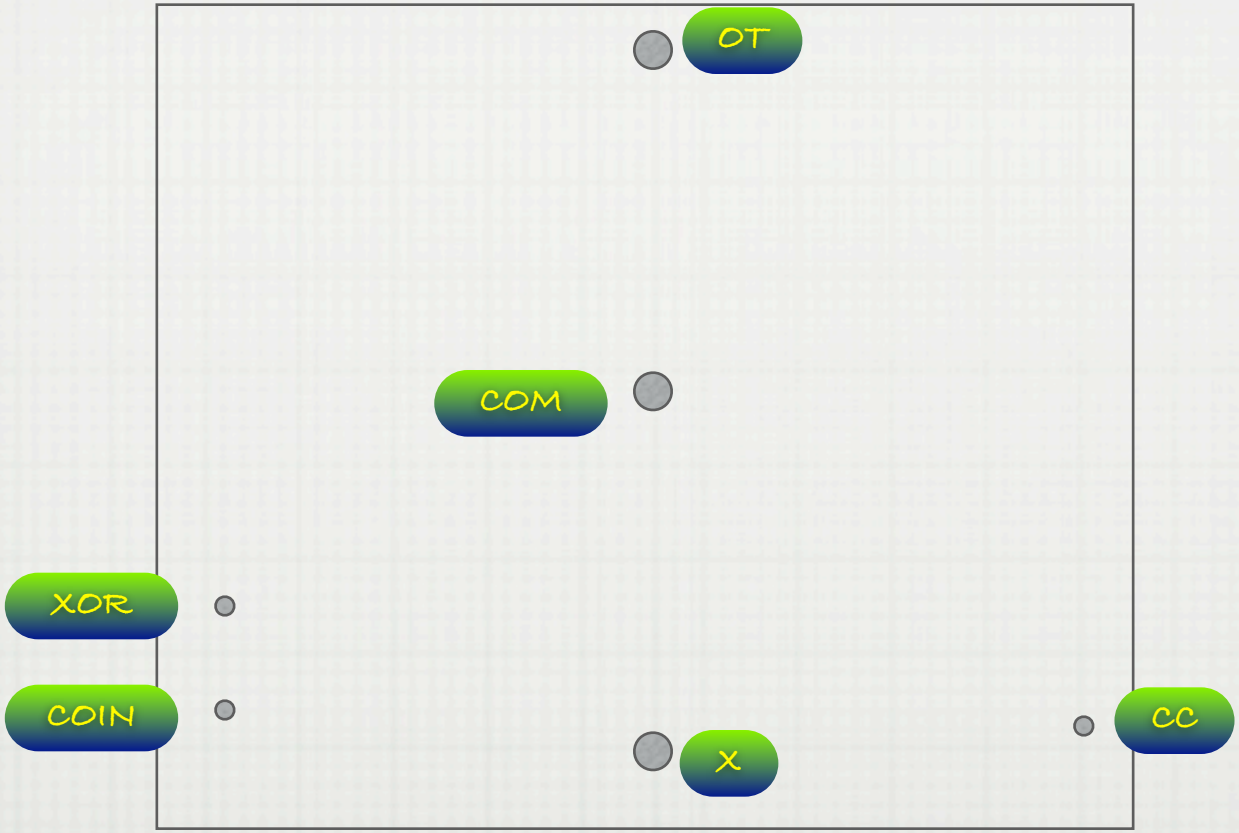
MPC FUNCTIONALITIES

- Different MPC functionalities encapsulate different ways one can "access" information
  - Access to learning information and influencing information
  - e.g. OT, key exchange, coin-tossing, commitment, ...
- Complexity: F reduces to G if there is a secure protocol for F using access to G (i.e., in G-hybrid)

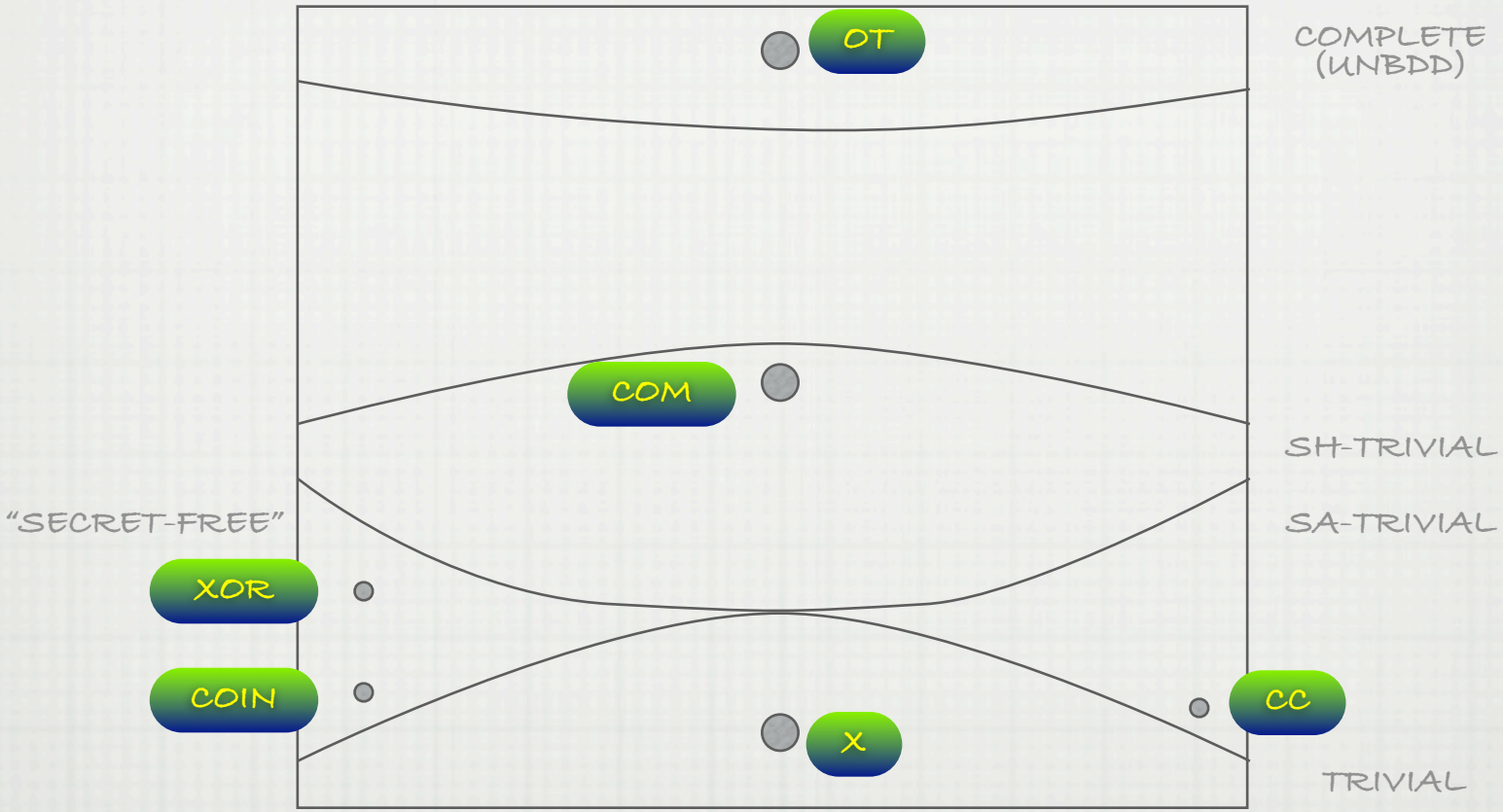
MPC FUNCTIONALITIES

- Different MPC functionalities encapsulate different ways one can "access" information
  - Access to learning information and influencing information
  - e.g. OT, key exchange, coin-tossing, commitment, ...
- Complexity: F reduces to G if there is a secure protocol for F using access to G (i.e., in G-hybrid)
  - "Cryptography" needed captures the gap between the kinds of information access in F and G

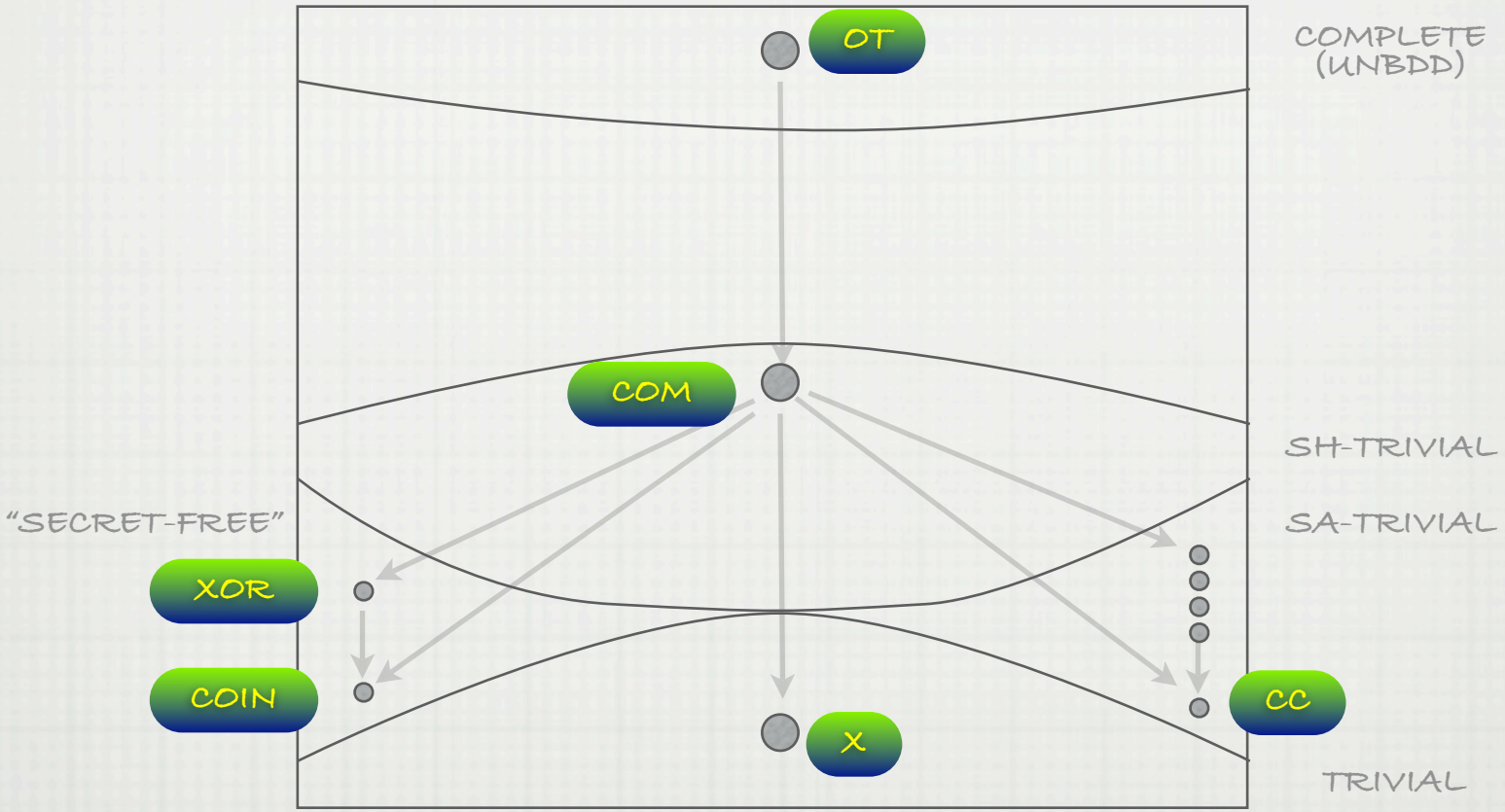
THE LANDSCAPE OF 2-PARTY FUNCTIONALITIES



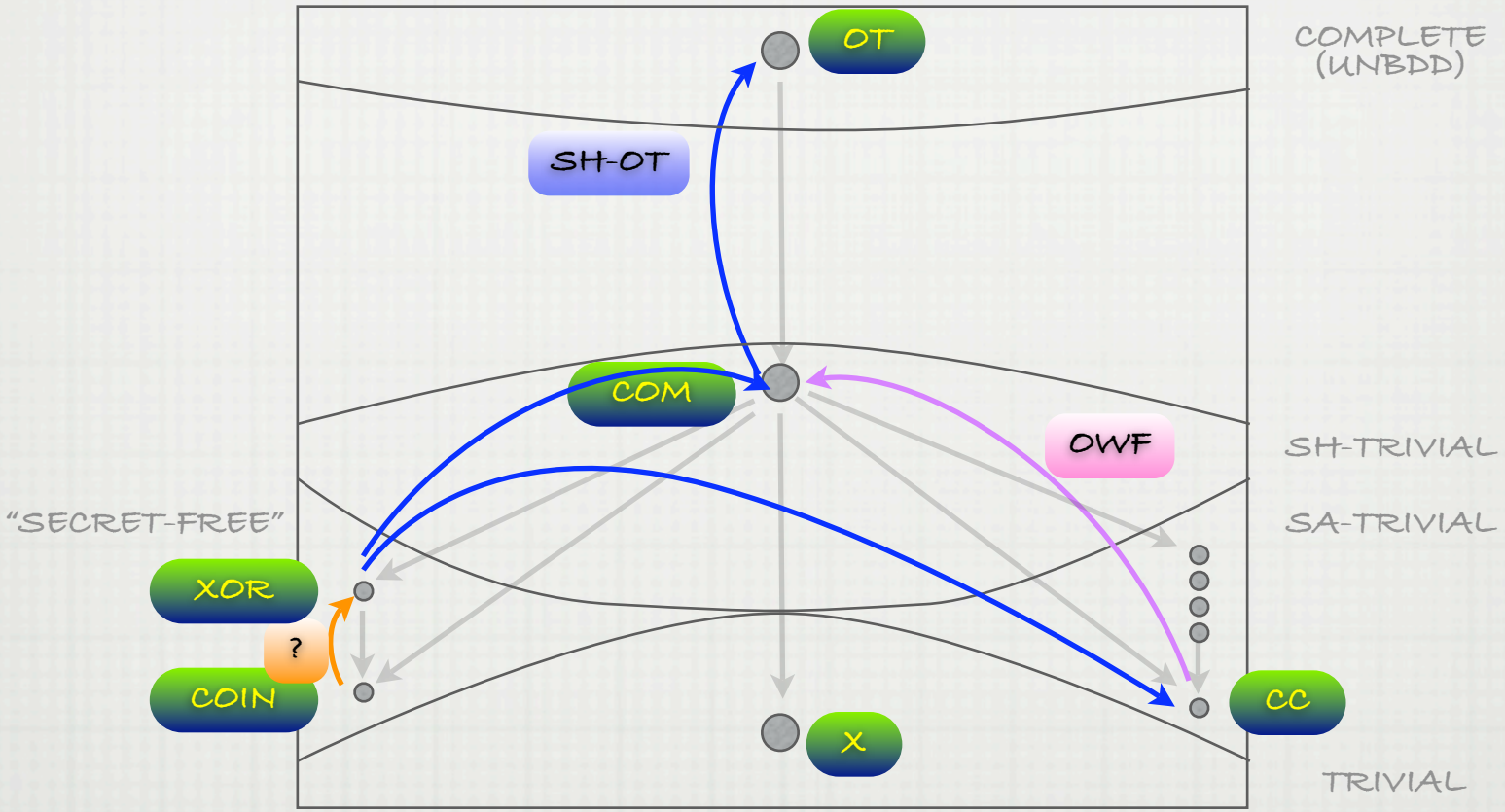
THE LANDSCAPE OF 2-PARTY FUNCTIONALITIES



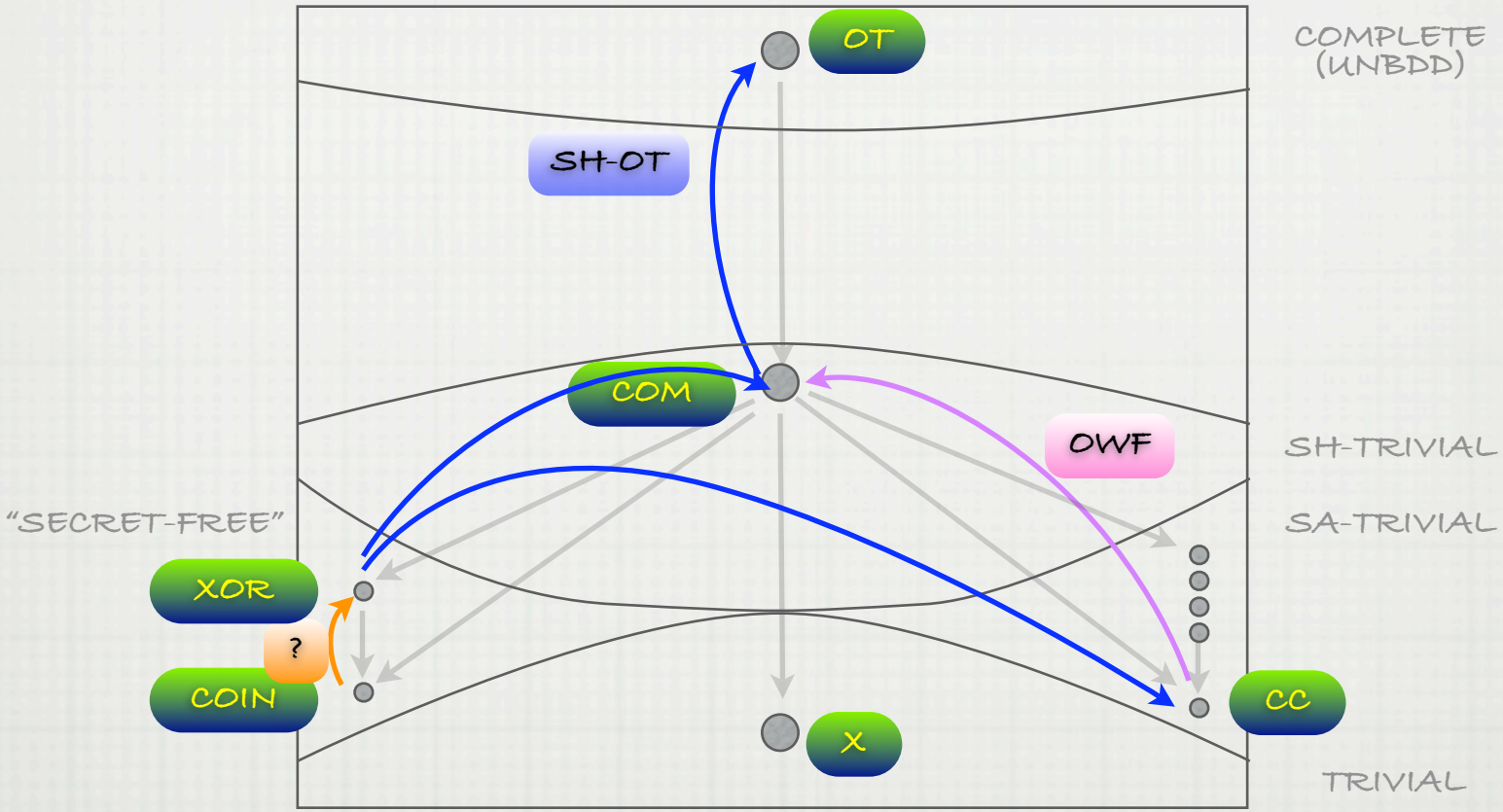
THE LANDSCAPE OF 2-PARTY FUNCTIONALITIES



THE LANDSCAPE OF 2-PARTY FUNCTIONALITIES

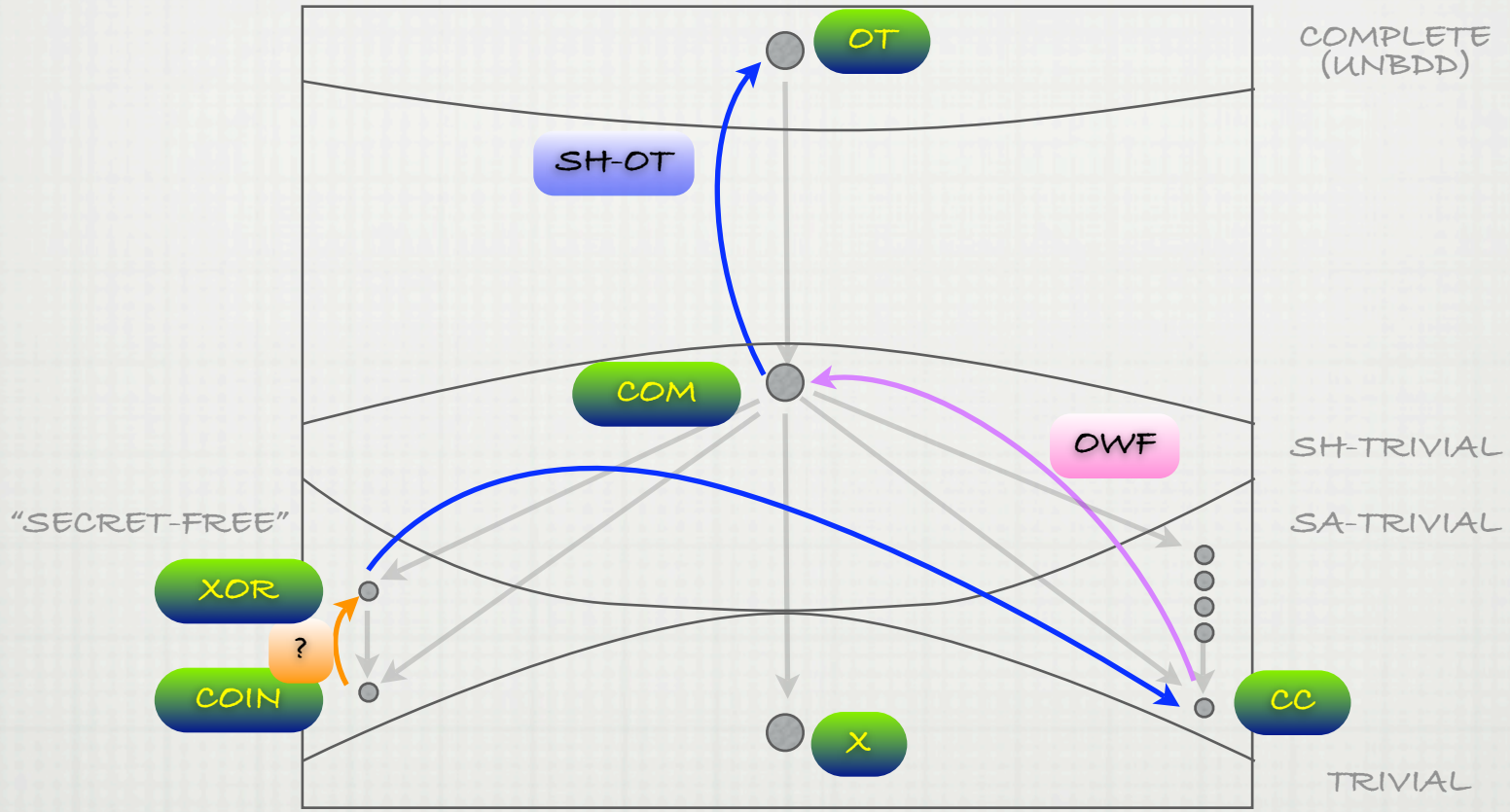


THE LANDSCAPE OF 2-PARTY FUNCTIONALITIES



- A Zero-One Law: If (and only if) sh-OT exists, every non-trivial functionality is complete!

THE LANDSCAPE OF 2-PARTY FUNCTIONALITIES

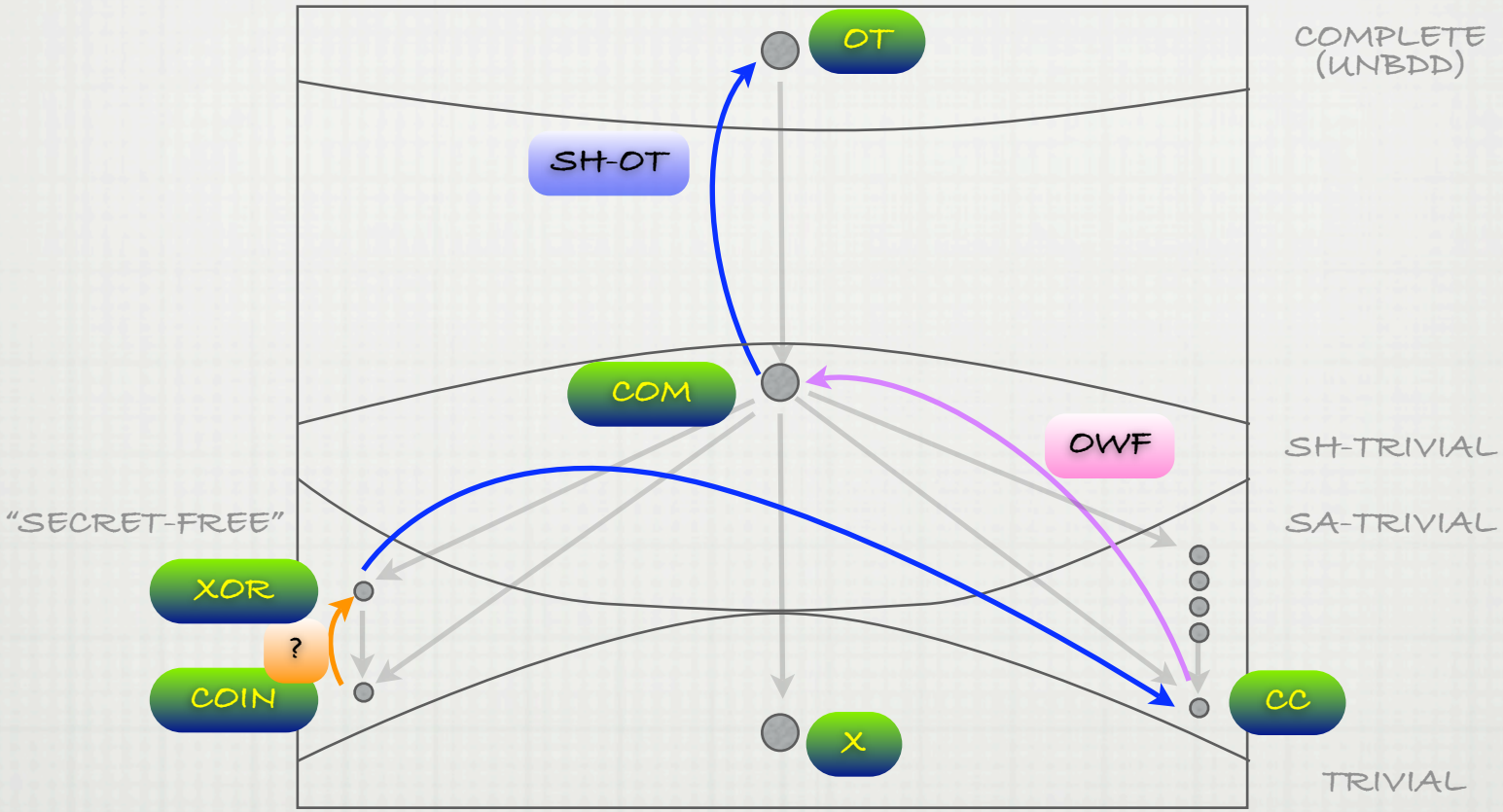


Algorithmica
Infinite hierarchy

Minicrypt (OWF)
Some collapses
(e.g. $F_{com} \sim F_{cc}$)

Cryptomania (sh-OT)
Zero-One Law

THE LANDSCAPE OF 2-PARTY FUNCTIONALITIES



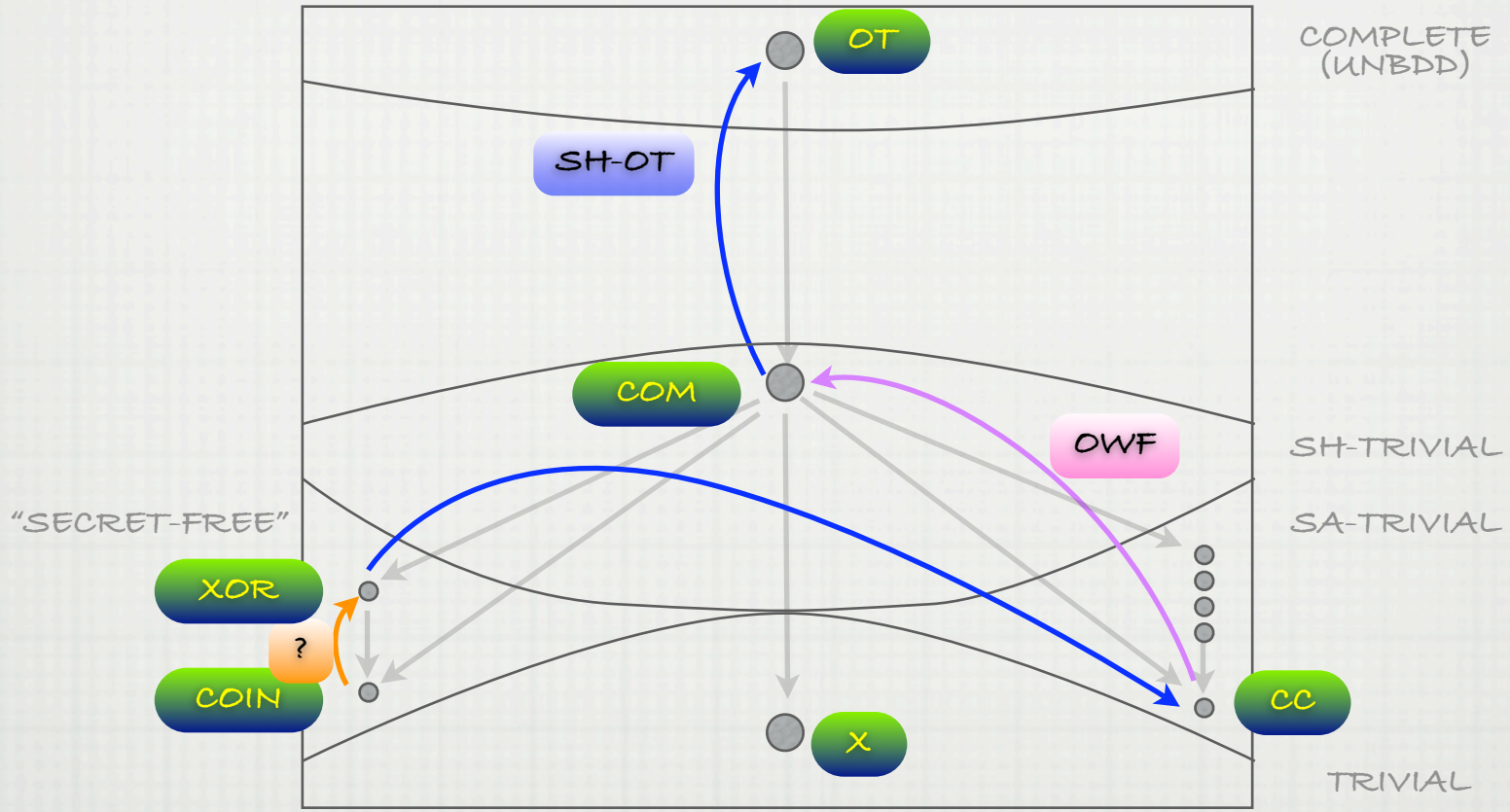
Algorithmica
Infinite hierarchy

Minicrypt (OWF)
Some collapses
(e.g. $F_{com} \sim F_{cc}$)

?

Cryptomania (sh-OT)
Zero-One Law

THE LANDSCAPE OF 2-PARTY FUNCTIONALITIES



- Conjecture [Finiteness of Assumption-Space]: The assumptions "F reduces to G" (over all pairs F,G) are only finitely many