509907.509980

- Universally Composable Two-Party and Multi-party Secure Computation
  - multi-party network
    - open communication
  - an adversary
    - corrupt as many parties as it wishes
  - securely realize
    - functionality
      - local inputs
    - under concurrent composition
    - unbounded num- ber of protocol executions
- stand-alone computation
  - doesnot
    - capture the security requirements
  - protocol
    - run concurrently with an unknown number of other protocols
    - unpredictable
- two-party functionalities
  - semi-honest (or, eavesdropping) ad- versaries
    - ideal Oblivi- ous Transfer (OT) functionality
    - show that the [33] construction, given access to the ideal OT functionality, can be used to securely realize any two-party ideal functional- ity in a universally composable way
  - transform any two-party protocol in the semi-honest model into a protocol that guarantees equivalent input-output relations in the presence of general, malicious adversaries
    - (UC) commitment protocol in the CRS model
    - plugging the new scheme into the UC zero-knowledge protocol of [12]
    - new ideal functionality, called commit-and-prove
    - cast the protocol compiler
      - compose
  - multi-party case
    - extend
      - extend the commitment
      - zero-knowledge
      - commit-and-prove
    - generalize the protocol compiler
- joint state
  - several protocol instances to use the same copy of the reference string
- Cryptographic assumptions
  - non-adaptive
    - trapdoor permutations
  - adaptive
    - additionally
      - obliviously generatable public-key encryption- schemes
- THE MODEL
  - ideal functionality
  - computation
    - an adversary, A,
    - simulator) S
    - parties
    - environment Z
      - generates the inputs
      - reads all outputs
      - interacts with the adversary

- 509907.509980
  - Universally Composable Two-Party and Multi-party Secure Computation (1)
    - multi-party network (1)
      - open communication (1)
    - an adversary (1)
      - corrupt as many parties as it wishes (1)
    - securely realize (1)
      - functionality (1)
        - local inputs (1)
      - under concurrent composition (1)
      - unbounded num- ber of protocol executions (1)
  - stand-alone computation (1)
    - doesnot (1)
      - capture the security requirements (1)
    - protocol (1)
      - run concurrently with an unknown number of other protocols (1)
      - unpredictable (1)
  - two-party functionalities (2)
    - semi-honest (or, eavesdropping) ad- versaries (2)
      - ideal Oblivi- ous Transfer (OT) functionality (2)
      - show that the [33] construction, given access to the ideal OT functionality, can be used to securely realize any two-party ideal functional- ity in a universally composable way (2)
    - transform any two-party protocol in the semi-honest model into a protocol that guarantees equivalent input-output relations in the presence of general, malicious adversaries (2)
      - (UC) commitment protocol in the CRS model (2)

- plugging the new scheme into the UC zero-knowledge protocol of [12] 2
- new ideal functionality, called commit-and-prove 2
- cast the protocol compiler 2
  - compose 2
- multi-party case 2
  - extend 2
    - extend the commitment 2
    - zero-knowledge 2
    - commit-and-prove 2
  - generalize the protocol compiler 2
- joint state 2
  - several protocol instances to use the same copy of the reference string 2
- Cryptographic assumptions 2
  - non-adaptive 2
    - trapdoor permutations 2
  - adaptive 2
    - additionally 2
      - obliviously generatable public-key encryption- schemes 2
- THE MODEL 3
  - ideal functionality 3
  - computation 3
    - an adversary, A, 3
    - simulator) S 3
    - parties 3

- environment Z 3
  - generates the inputs 3
  - reads all outputs 3
  - interacts with the adversary 3