An overview of Topology-Hiding Computation

Daniel Tschudi, Aarhus University
Social Network

‘Trusted’ Party

computes functions on data & graph
controls all information on data & graph

Goal: Decentralized Network

computation without trusted party
data & graph are private information
Multi-Party Computation

Network topology must be public for MPC!

Network topology = sensitive information
THC := MPC where graph and inputs are private.
Model & Security
Network Model

An incomplete network of synchronous, secure channels.
Network Model

**Honest party** knows its **neighbourhood**

*incomplete* network of synchronous, secure channels
Network Model

**incomplete** network of synchronous, secure channels

**Adversary** knows joint neighbourhood of corrupted parties
Security Definition

- **game-based** security (IND-CTA)
- **simulation-based** security
Security Definition

\[ \forall G \in \mathcal{G} \quad \pi_G \quad \mathcal{N}_G \xrightarrow{\pi_G} \mathcal{F}, \mathcal{N}_G \]

network functionality

graph class, e.g. connected graphs

target functionality

Simulation

Simulation-based security
Information-Theoretic Setting

- No THC protocol without (significant) leakage exists. [HJ07]

Fail-stop Adversary

- No THC protocol without leakage exists. [MOR15]

Semi-honest Adversary

- THC BC implies OT. [BBMM18]
Feasibility Results

- Computationally bounded, $t < n$
- Semi-honest
  - Full-security
    - No leakage
- Fail-stop
  - Security w. abort
    - Small leakage
- Arbitrary connected graphs
- DDH or QR or LWE
  - Or OWF + secure hardware

References:

- [MOR15], [HMTZ16], [AM17], [ALM17], [BBMM18], [LLM+18]
Topology-Hiding Protocol Design for the semi-honest case
Topology-Hiding Protocol Design

Topology Hiding MPC
Topology-Hiding Protocol Design

Topography-Hiding OR gives broadcast in the semi-honest case
**Goal:** Compute OR

**Protocol:** In each round exchange bits and locally compute the OR.
Goal: Compute OR

Protocol: In each round exchange bits and locally compute the OR.
**Goal:** Compute OR

**Protocol:** In each round exchange bits and locally compute the OR.
Goal: Compute OR

Protocol: In each round exchange bits and locally compute the OR.
**Goal:** Compute OR

**Protocol:** In each round exchange bits and locally compute the OR.
**Goal:** Compute OR

**Protocol:** In each round exchange bits and locally compute the OR.
First Attempt

Goal: Compute OR

Protocol: In each round exchange bits and locally compute the OR.

Protocol leaks distances!
Sources of Leakage

message pattern

message content
Topology-Hiding Protocol Design

Topology Hiding OR
Design Approaches

Flooding [HMTZ16]

(Random) Walks [AM17, ALM17]
For each party collect the information along a random walk.

Hide the message pattern by executing random walks in parallel.

Hide the message content using encryption.
Onion Encryption

Homomorphic Public-Key Encryption

\[ pk \xleftarrow{} \text{KeyGen} \rightarrow sk \]

\[ m \xrightarrow{} \text{Enc} \rightarrow [m]_{pk} \xrightarrow{} \text{Dec} \rightarrow m \]

homomorphic: \[ [m_1]_{pk} \cdot [m_2]_{pk} = [m_1 + m_2]_{pk} \]

allowing for layered encryption

achievable from DDH, QR, LWE
**Goal:** Compute OR within encryptions

\[ [b_1]_{pk} \odot [b_2]_{pk} = [b_1 \lor b_2]_{pk} \]

**Problem:** We have

\[ [m_1]_{pk} \cdot [m_2]_{pk} = [m_1 + m_2]_{pk} \]

**Solution:** Encode bit b

\[
\begin{cases}
[0]_{pk} & \text{if } b = 0 \\
[r]_{pk} & \text{if } b = 1 \text{ for (r random)}
\end{cases}
\]

to get **OR-homomorphism.**
Example: Compute OR on a Path

Encrypted OR
Random Walk Protocol:
- Parties start \textit{walks} in all directions
- In each round \textit{permute walks}
- Compute \textit{OR} along each walk

Correctness:
- requires \textit{random walks} to \textit{cover} the graph

Topology-hiding:
- \textit{message pattern} is \textit{independent} of the graph
- \textit{message content} hidden using onion encryption
Random Walk

The problem with fail-stops
Topology-Hiding Protocol Design

Standard MPC

Topology-Hiding OR
Open Problems

- THC for Dynamic Networks
- vehicular networks
- THC secure against active adversary
- Asynchronous THC
- Honest Majority THC
- Practical THC - the next TOR
- Lower Bounds on communication complexity
- Adaptive Corruption
Literature

- **[MOR15]**

- **[HMTZ16]**
  Martin Hirt, Ueli Maurer, Daniel Tschudi, Vassilis Zikas, *Network-hiding communication and applications to multi-party protocols*, CRYPTO’16

- **[AM17]**

- **[BBMM18]**

- **[LLM+18]**

- **[HJ07]**
  M. Hinkelmann and A. Jakoby, *Communications in unknown networks: Preserving the secret of topology*, 2007