Compact Adversary Structures

Martin Hirt
ETH Zurich

Theory and Practice of MPC, Aarhus, May 2016

Motivation II

Threshold-Adversary Setting
- Characterization: \( n, t \in \mathbb{N} \)
- E.g.: \( n = 7, t = 3 \)
  \[ Z = \{ (\text{Cinderella}, \text{Depp}), (\text{Peggie}, \text{Dumbo}), \ldots \} \]
- Complexity of MPC: \( \text{Polyn}(n, 1) \)

General-Adversary Setting
- Characterization: \( \mathcal{P} \) with \( |\mathcal{P}| = n \) \( Z \subseteq 2^\mathcal{P} \)
- E.g. \( \mathcal{P} = \{ (\text{Cinderella}, \text{Depp}), (\text{Peggie}, \text{Dumbo}), \ldots \} \)
- Complexity of MPC: \( \text{Polyn}(|\mathcal{P}|, |Z|) = \text{Exp}(n) \)

However: For "natural" \( Z \), size \( |Z| \in \text{Exp}(n) \)

Outline

- General Adversaries: The Basics
- \( \forall \) constructions \( \exists \) adversary structures \( Z \) s.t. \( |\pi_Z| \in \text{Exp}(n) \)
- MPC for Adversary Structures (recap)
- MPC for Delta Structures
- Conclusions

Notation

- Party set \( \mathcal{P} \), \( |\mathcal{P}| = n \) here: \( \mathcal{P} = [n] \) (Adv. chooses one of them)
- Monotone adversary structure \( Z = \{ Z_1, Z_2, \ldots, Z_\ell \} \subseteq 2^\mathcal{P} \)
  \footnotesize{(Monotone: \( Z \subseteq Z' \) \( \Rightarrow \) \( Z \subseteq Z' \))}

Definitions

- \( Q^t(P, Z) \) \( : \Leftrightarrow \forall Z_1, Z_2 \in Z: Z_1 \cup Z_2 \neq \mathcal{P} \) (no two sets add up to \( \mathcal{P} \))
- \( Q^t_{\text{max}}(P, Z) \) \( : \Leftrightarrow Q^t(P, Z) \land \exists Z' \subseteq Z : Q^t(P, Z') \) (bigger \( Z' \) are not \( Q^t \))

Results

- I.T. passive, crypto. active: \( t < n/2 \) \( Q^t(P, Z) \)
- I.T. active: \( t < n/3 \) \( Q^t(P, Z) \)
- Asynchronous, perfect: \( t < n/4 \) \( Q^t(P, Z) \)

Lessem, north, guidon, nemo, \( \text{Polyn}, \text{Exp} \), 

Length of GA MPC Protocols – Roadmap

Lemma: \( \forall \) constructions \( \exists \) adversary structures \( Z \) s.t. \( |\pi_Z| \in \text{Exp}(n) \)

Proof Roadmap
1. Count maximal adversary structures for given \( n \) (lower bound)
2. Derive length of GA MPC protocols (for some adversary structures)
Outline

• General Adversaries: The Basics
• \forall constructions \exists adversary structures \mathcal{Z} s.t. |\pi_{\mathcal{Z}}| \in \text{Exp}(n)
  - MPC for Adversary Structures (recap)
  - MPC for Delta Structures
  - Conclusions

Counting Q^2-Maximal Adversary Structures

Idea of Construction
\[ n \text{ even, } t = n/2 - 1, \quad i.e., \quad t + 1 = n/2 \]

Construction
1. Fix \( \mathcal{P} = [n] \) with \( n \) even, let \( t = n/2 - 1 \), and \( \mathcal{Z} = \{ \mathcal{Z} \subseteq \mathcal{P} : |\mathcal{Z}| \leq t \} \).

Counting Q^2-Maximal Adversary Structures (continued)

Construction
2. Let \( B = (B_1, B_2, \ldots, B_\ell) := \{ B \subseteq [n-1] : |B| = t+1 \} \).

Claim: \( \forall Z \subseteq \mathcal{P}, |Z| = t+1 \text{ : } (Z \in B) \text{ or } (Z^c \in B) \).

Proof:
A) If \( n \notin \mathcal{Z} \), then \( Z \in B \).
B) Otherwise, \( Z^c \) is a \( (t+1) \)-subset of \( P \) with \( n \notin Z^c \), hence \( Z^c \in B \).

Proof of Q^2:
Consider \( Z_1, Z_2 \in Z \), then...
A) \( Z_1 \in Z \text{ or } Z_2 \in Z : |Z_1| + |Z_2| < n. \)
B) \( Z_1, Z_2 \in B : \exists i, j : Z_1 = B_i, Z_2 = B_j \) and \( i \neq j \Rightarrow B_i \neq B_j \cup Z, B_j \neq B_i \cup Z \).

Proof of Maximality: Consider \( Z \) to be appended to \( \hat{Z} \), then...
A) \( |\hat{Z}| \leq t : Z \) is already contained in \( \hat{Z} \).
B) \( |\hat{Z}| \geq t+2 : Z^c \) is in \( \hat{Z} \), hence \( \hat{Z} \cup \{Z\} \) violates Q^2.
C) \( |\hat{Z}| = t+1 : \exists Z \in B \) (contained), or \( Z^c \in B \) (violates Q^2).

Counting Q^2-Maximal Adversary Structures (continued)

Analysis
\[ \ell = \binom{n-1}{t+1} \geq 2^t = 2^{n/2-1} \]

There are (at least) \( 2^{n/2-1} \) different Q^2-maximal adversary structures.
### MPC: Classic View

![MPC: Classic View Diagram]

#### Security Statement
What Adv can achieve in Real, she can also achieve in Ideal, while corrupting the same users (and never `g`).

#### Limitations
- Implicit assumption: Ideal is “good” if and only if `g` is honest.
- Guarantees only if few enough players are corrupted → example.

### MPC: Modern View

![MPC: Modern View Diagram]

#### Security Statement
What Adv can achieve in Ideal World, she can also achieve in Real World, assuming: Ideal is “good” if and only if `g` is honest.

### Construction
- Given `P`, all sets `Z ⊆ P` with `|Z| < |P|/2` are tolerated “for free”.
- Specify delta structure `ΔZ` with additional (larger) sets `Z`.
- Automatically “removes” incompatible small sets `Z`.

#### Definitions
- **Delta Structure** `ΔZ = (Z₁, Z₂, ⋯, Zₙ) ⊆ 2^P` (usually not monotone)
- **Monotone Closure** `Δ(Z) := \{Z ⊆ P | \exists Z' ∈ Δ(Z) : Z ⊆ Z'\}` (include subsets)

#### Security
- Secure against delta structure `ΔZ` implies secure against adversary structure `Δ(Z)`.

### MPC for General Adversary Structures

#### Given
- Threshold 3-PC Protocol secure for Player Simulation ([BGW] does the job)
- Target `(P, Δ(Z))` with `Q^2(P, Δ(Z))` (to be constructed).

#### Construction
A) `|Z| ≤ 2`: There is a trusted party `∃P_1 ∈ P`.
B) If `|Z| ≥ 3`:
   1. Partition `Z` into `Z₁, Z₂, Z₃` of similar size.
   2. Construct MPC protocols `Δ`, for each `Z′ = Z \ \ Z_i`.
   3. Let `P₁`, `P₂`, `P₃` run threshold MPC with `n = 3, t = 1`.

#### Analysis
- Every `Z ∈ Z` is contained in two `Z′` → these parties behave honestly in threshold MPC → honest majority.
- Efficiency: `Exp(recursion depth) = Exp(log(|Z|)) = Poly(|Z|)`.

### Delta Structures

#### Intuition
- Given `P`, all sets `Z ⊆ P` with `|Z| < |P|/2` are tolerated “for free”.
- Specify delta structure `ΔZ` with additional (larger) sets `Z`.
- Automatically “removes” incompatible small sets `Z`.

#### Definitions
- **Delta Structure** `ΔZ = (Z₁, Z₂, ⋯, Zₙ) ⊆ 2^P` (usually not monotone)
- **Monotone Closure** `Δ(Z) := \{Z ⊆ P | \exists Z' ∈ Δ(Z) : Z ⊆ Z'\}` (include subsets)
- **Enforced add** `Z₁ ∪ Z₂ := \{Z ∈ Z₁ | Z' ∉ Z₂\} ∪ Z₂`
- **Induced structure** `Δ(Z) := \{Z ∈ P | |Z| < |P|/2\} ∪ Δ(Z)`

#### Security
- Secure against delta structure `ΔZ` implies secure against adversary structure `Δ(Z)`.

### MPC for Delta Structures

#### Given
- Threshold `n`-PC Protocol secure for Player Simulation ([BGW] does the job).
- Target `(P, Δ(Z))` with `Q^2(P, Δ(Z))` (to be constructed).

#### Construction
A) `|Δ(Z)| ≤ 2`: See next slides.  
B) If `|Δ(Z)| ≥ 3`:
   1. Partition `Δ(Z)` into `Δ(Z₁), Δ(Z₂), Δ(Z₃)` of similar size.
   2. Construct MPC protocols `Δ`, for each `Δ(Z)' = Δ(Z) \ Δ(Z)`.  
   3. Let `P₁`, `P₂`, `P₃` run threshold MPC with `n = 3, t = 1`.

#### Analysis
- Every `Z ∈ Δ(Z)` is contained in two `Δ(Z)'` → honest majority.
- Efficiency: `Exp(recursion depth) = Exp(log(|Δ(Z)|)) = Poly(|Δ(Z)|)`.

### MPC for Delta Structures (cont’d)

#### Adding one Adversary Set
- Given: `if` for `P, Z` with `Q^2(P, Z)` and an additional set `Z₁ ⊆ P`.
- Goal: Construct `#` for `P, (Z ∪ \{Z₁\})`.

#### Construction
A) `Z₁` is sufficient:  
\[Z₁ \text{ is sufficient}\]

\[P = \{P₁, P₂, \ldots, Pₙ\}, k = \{Z₁\} \text{ (honest parties in } Z₁)\].

1. `P₁ = \{P₁, P₂, \ldots, Pₙ\}`, tolerating `k-1` corruptions.
   - `k` parties
   - `k = 1` copies of `P_i`

#### Lemma: The above construction is secure against `(Z ∪ \{Z₁\})`.

#### Proof:
Consider `Z ∈ (Z ∪ \{Z₁\})`.
A) Suppose `Z ∈ Z, Z ∪ Z₁ ≠ P`. The simulations of honest `P₁`’s have honest majority.
B) Suppose `Z = Z₁`. All `P_i` in `Z` are correctly simulated!

#### Efficiency: `Poly(n)` blow-up on for additional set `Z₁`.

---

### Outline

- General Adversaries: The Basics
- `∀` constructions 3 adversary structures `Z` s.t. `|π| ∈ Exp(n)`
- MPC for Adversary Structures (recap)
- MPC for Delta Structures
- Conclusions
Adding multiple Adversary Set

- Given: $\pi$ for $P, Z$ and $k$ additional sets $Z_1, \ldots, Z_k \subseteq P$.
- Goal: Construct $\pi'$ for $P, (Z \cup \{Z_1, \ldots, Z_k\})$.

Construction

- Add sets one-by-one (in $k$ steps)

Efficiency: $\exp(k)$ blow-up for $k$ additional sets $Z_1, \ldots, Z_k$.

Putting Things Together

- $\log(|\Delta Z|)$ recursion steps for $\Delta Z$, 2 recursion steps for threshold structure.
- Overall complexity: $\exp(\log(|\Delta Z|) + 2) = \text{Poly}(|\Delta Z|)$.

Conclusions

What we achieved

- Poly-time protocols for delta-structures
- Captures all adversary structures, efficient for "close-to-threshold"

What we missed

- Efficient protocols for delta-structures

What is Open

- Other description languages?