Compact Adversary Structures

Martin Hirt

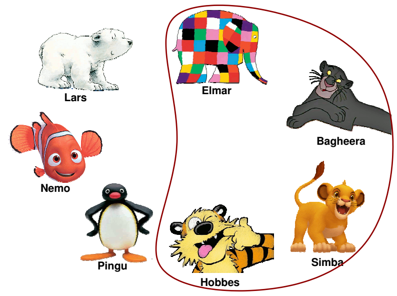
ETH Zurich

Theory and Practice of MPC, Aarhus, May 2016

Motivation I

Threshold [GMW,BGW,CCD,...]
Condition: < half corrupted

General Adversaries [HM,SS,CDM,...]
Condition: $\text{set}_i \cup \text{set}_j \neq$ all parties



Motivation II

Threshold-Adversary Setting

- Characterization: $n, t \in \mathbb{N}$
  E.g.: $n = 7$, $t = 3$
- $\boxed{\text{Complexity of MPC: Poly}(n, t)}$

General-Adversary Setting

- Characterization: $\mathcal{P}$ with $|\mathcal{P}| = n$, $\mathcal{Z} \subseteq 2^{\mathcal{P}}$

  E.g. $\mathcal{P} = \{$  $\}$,

  $\mathcal{Z} = \Big\{ \{$  $\}, \{$  $\}, \dots \Big\}$
- $\boxed{\text{Complexity of MPC: Poly}(|\mathcal{P}|, |\mathcal{Z}|)} = \boxed{\text{Exp}(n)}$

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

Motivation III

Summary

- Threshold MPC: Poly(n) [GMW,BGW,CCD,RB,Bea,CDN,...]
- General MPC: Exp(n) [HM,SS,CDM,Mau,HT,...]

Resorts

- Find more efficient GA protocols
  $\Rightarrow$ $\forall$ constructions $\exists$ adversary structures $\mathcal{Z}$ s.t. $|\pi_{\mathcal{Z}}| \in \text{Exp}(n)$
- Find constructions s.t. $\forall$ natural $\mathcal{Z}$: $|\pi_{\mathcal{Z}}| \in \text{Poly}(n)$

  Formally: Description language L, s.t.

	Threshold	Adv.Strucs	Delta Strucs
– Completeness: $\forall \mathcal{Z} \subseteq 2^{\mathcal{P}}\ \exists D \in L : D \sim \mathcal{Z}$	✗	✓	✓
– Naturalness: "natural" $\mathcal{Z}$ have small descriptions D	✓	✗	✓
– Efficiency: $\forall D \in L\ \exists \pi_D : |\pi_D| = \text{Poly}(n, |D|)$	✓	✓	✓

Today: Delta Structures = Close-to-Threshold Adversary Structures

Outline

- $\boxed{\text{General Adversaries: The Basics}}$
- $\forall$ 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

Notation and Results

Notation

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

Definitions

- $Q^2(\mathcal{P}, \mathcal{Z}) :\Leftrightarrow \forall Z_1, Z_2 \in \mathcal{Z} : Z_1 \cup Z_2 \neq \mathcal{P}$ (no two sets add up to $\mathcal{P}$)
- $Q^2_{\text{max}}(\mathcal{P}, \mathcal{Z}) :\Leftrightarrow Q^2(\mathcal{P}, \mathcal{Z}) \wedge \nexists \mathcal{Z}' \supsetneq \mathcal{Z} : Q^2(\mathcal{P}, \mathcal{Z}')$ (bigger $\mathcal{Z}'$ are not Q^2)

Results

	Threshold	Gen.Adv.
• I.T. passive, crypto. active:	$t < n/2$	$Q^2(\mathcal{P}, \mathcal{Z})$
• I.T. active:	$t < n/3$	$Q^3(\mathcal{P}, \mathcal{Z})$
• Asynchronous, perfect	$t < n/4$	$Q^4(\mathcal{P}, \mathcal{Z})$

Outline

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

Length of GA MPC Protocols – Roadmap

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

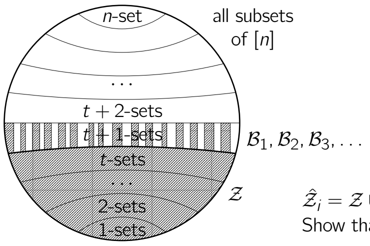
Proof Roadmap

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

Counting Q^2-Maximal Adversary Structures

Idea of Construction

n even, $t = n/2 - 1$, i.e., $t + 1 = n/2$



$\hat{\mathcal{Z}}_i = \mathcal{Z} \cup \mathcal{B}_i$
Show that $\hat{\mathcal{Z}}_i$ is Q^2-maximal

Counting Q^2-Maximal Adversary Structures

Construction

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

Counting Q^2-Maximal Adversary Structures (continued)

Construction

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

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

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

Claim: $\widehat{\mathcal{Z}} := (\mathcal{B} \cup \mathcal{Z})$ is Q^2_{max}.

Proof of Q^2: Consider $Z_1, Z_2 \in \widehat{\mathcal{Z}}$, then ...
A) $Z_1 \in \mathcal{Z}$ or $Z_2 \in \mathcal{Z}$: $|Z_1| + |Z_2| \leq t + (t+1) < n$.
B) $Z_1, Z_2 \in \mathcal{B}$: $n \notin (Z_1 \cup Z_2)$.

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

Counting Q^2-Maximal Adversary Structures (continued)

Construction

3. For binary vector $\vec{x}$ of length ℓ, let

$$\mathcal{B}_{\vec{x}} := \{B_1', B_2', \ldots, B_\ell'\}, \text{ where } B_i' = \begin{cases} B_i, & \text{if } x_i = 0 \\ B_i^c, & \text{if } x_i = 1 \end{cases}$$

Claim: $\widehat{\mathcal{Z}}_{\vec{x}} := (\mathcal{B}_{\vec{x}} \cup \mathcal{Z})$ is Q^2_{max} for any $\vec{x}$.

Proof of Q^2: Consider $Z_1, Z_2 \in \widehat{\mathcal{Z}}_{\vec{x}}$, then ...
A) $Z_1 \in \mathcal{Z}$ or $Z_2 \in \mathcal{Z}$: $|Z_1| + |Z_2| < n$.
B) $Z_1, Z_2 \in \mathcal{B}_{\vec{x}}$: $\exists i, j : Z_1 = B_i' \;\wedge\; Z_2 = B_j'$
$i \neq j \;\Rightarrow\; B_i \neq B_j \;\wedge\; B_i \neq B_j^c \;\Rightarrow\; Z_1 \cup Z_2 \neq \mathcal{P}$.

Proof of Maximality: Consider Z to be appended to $\widehat{\mathcal{Z}}_{\vec{x}}$, then ...
A) $|Z| \leq t$: Z is already contained in $\widehat{\mathcal{Z}}_{\vec{x}}$.
B) $|Z| \geq t + 2$: Z^c is in $\mathcal{Z}$, hence $\widehat{\mathcal{Z}}_{\vec{x}} \cup \{Z\}$ violates Q^2.
C) $|Z| = t + 1$: $\exists i : Z = B_i \;\vee\; Z = B_i^c$.
One of them is already in $\widehat{\mathcal{Z}}_{\vec{x}}$, the other would violate Q^2.

Counting Q^2-Maximal Adversary Structures (continued)

Analysis

- $\ell = \binom{n-1}{t+1} = \dfrac{(n-1) \cdot (n-2) \cdot \ldots \cdot (n-t)}{t \quad \cdot (t-1) \cdot \ldots \cdot \quad 1} \geq 2^t = 2^{n/2-1}$
- There are (at least) $2^{2^{n/2-1}}$ different Q^2-maximal adversary structures.

Length of GA MPC Protocols

Lemma: Let $\mathcal{Z}_1 \neq \mathcal{Z}_2$ be Q^2-maximal adversary structures (for some $\mathcal{P}$). Then $\pi_{\mathcal{Z}_1} \neq \pi_{\mathcal{Z}_2}$

Proof: Otherwise, there would be secure for $\mathcal{Z}_1 \cup \mathcal{Z}_2$, which is not Q^2.

Theorem: $\exists$ adversary structures $\mathcal{Z}$ s.t. $|\pi_{\mathcal{Z}}| \in \text{Exp}(n)$

Proof: There are $2^{2^{n/2-1}}$ different Q^2-maximal adversary structures, each requiring a different π. Hence, some π have length at least $2^{n/2-1}$.

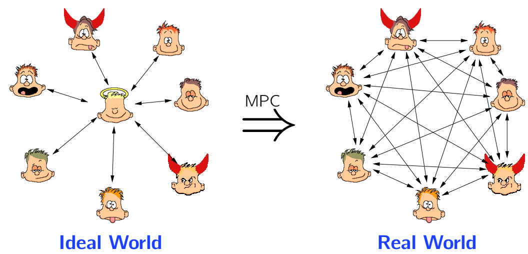
Corollary: Same holds in the Q^3 and the Q^4 worlds ...

Note: Does not (necessarily) imply exponential communication.

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

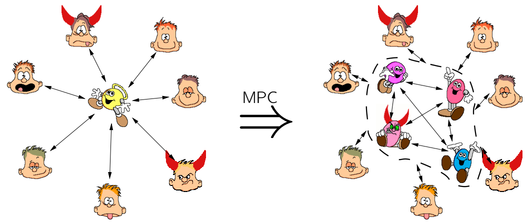
MPC: Ancient View



Security Statement:
What Adv can achieve in Real, she can also achieve in Ideal, *while corrupting the same parties.*

Limitation: Parties with inputs/outputs $\equiv$ computing parties.

MPC: Classic View



Ideal World **Real World**

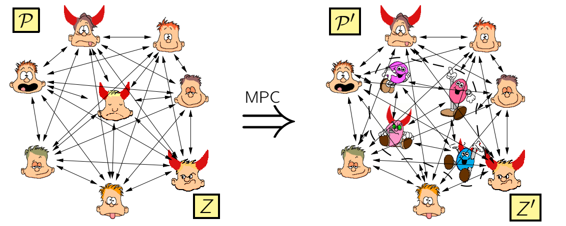
Security Statement

What Adv can achieve in Real, she can also achieve in Ideal, *while corrupting the same users (and never*).

Limitations

- Implicit assumption: Ideal is "good" if and only if is honest.
- Guarantees only if few enough players are corrupted → example.

MPC: Modern View



~~Ideal World~~ **Prot.** $\bar{\pi}$ ~~Real World~~ **Prot.** $\bar{\pi}'$

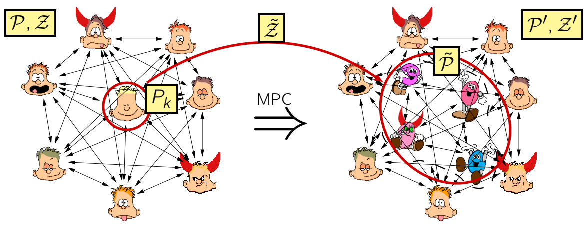
Security Statement

What Adv can achieve in $\bar{\pi}'$, she can also achieve in $\bar{\pi}$, while corrupting $Z = Z' \cap \mathcal{P}$.

Additional Security Requirement

- Too much cheating → is dishonest (but not worse).
- Achieved by [BGW], and probably all others ...

MPC: Player Simulation



Protocol $\bar{\pi}$ **Protocol** $\bar{\pi}'$

Deriving Adversary Structure

- Assume: $\bar{\pi}$ (for $\mathcal{P}$) is "good" when attacked by some Adv in $\mathcal{Z}$.
- Simulate $P_k \in \mathcal{P}$ with an MPC protocol among $\tilde{\mathcal{P}}$ secure against $\tilde{\mathcal{Z}}$.
- Then $\mathcal{P}' = (\mathcal{P} \setminus \{P_k\}) \cup \tilde{\mathcal{P}}$, and

$$\mathcal{Z}' = \left\{ Z' \subseteq \mathcal{P}' \;\middle|\; \begin{array}{l} (Z' \cup \{P_k\}) \cap \mathcal{P} \in \mathcal{Z} \quad \bigvee \\ (Z' \setminus \{P_k\}) \cap \mathcal{P} \in \mathcal{Z} \quad \wedge \; (Z' \cap \tilde{\mathcal{P}}) \in \tilde{\mathcal{Z}} \end{array} \right\}$$

MPC for General Adversary Structures [HM]

Given

- Threshold 3-PC Protocol secure for Player Simulation ([BGW] does the job)
- Target $\mathcal{P}, \mathcal{Z}$ with $Q^2(\mathcal{P}, \mathcal{Z})$ (to be constructed).

Construction

A) $|\mathcal{Z}| \leq 2$: There is a trusted party $\exists P_j \in \mathcal{P}$.

B) If $|\mathcal{Z}| \geq 3$:

1. Partition $\mathcal{Z}$ into $\mathcal{Z}_1, \mathcal{Z}_2, \mathcal{Z}_3$ of similar size.
2. Construct MPC protocols $\bar{\pi}_i$ for each $\mathcal{Z}_i^c = \mathcal{Z} \setminus \mathcal{Z}_i$. (recursion)
3. Let $\bar{\pi}_1, \bar{\pi}_2, \bar{\pi}_3$ run threshold MPC with $n = 3$, $t = 1$.

Analysis

- Every $Z \in \mathcal{Z}$ is contained in two $\mathcal{Z}_i^c$
  → these parties behave honestly in threshold MPC → honest majority.
- Efficiency: Exp(recursion depth) = Exp(log($|\mathcal{Z}|$)) = Poly($|\mathcal{Z}|$).

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

Delta Structures

Intuition

- Given $\mathcal{P}$, all sets $Z \subseteq \mathcal{P}$ with $|Z| < |\mathcal{P}|/2$ are tolerated "for free".
- Specify delta structure $\Delta\mathcal{Z}$ with additional (larger) sets Z.
- Automatically "removes" incompatible small sets Z.

Definitions

- Delta Structure $\Delta\mathcal{Z} = \{Z_1, Z_2, \ldots, Z_\ell\} \subseteq 2^{\mathcal{P}}$ (usually not monotone)
- Monotone Closure $\langle\Delta\mathcal{Z}\rangle := \{Z \subseteq \mathcal{P} \mid \exists Z' \in \Delta\mathcal{Z} : Z \subseteq Z'\}$ (include subsets)
- Enforced add $\mathcal{Z}_1 \cup_! \mathcal{Z}_2 := \{Z \in \mathcal{Z}_1 \mid Z^c \notin \mathcal{Z}_2\} \cup \mathcal{Z}_2$
- Induced structure $\Delta^{\!*}\mathcal{Z} := \{Z \in \mathcal{P} : |Z| < |\mathcal{P}|/2\} \cup_! \langle\Delta\mathcal{Z}\rangle$

Security

- Secure against delta structure $\Delta\mathcal{Z}$:≡ secure against adversary structure $\Delta^{\!*}\mathcal{Z}$.

MPC for Delta Structures

Given

- Threshold n-PC Protocol secure for Player Simulation ([BGW] does the job).
- Target $(\mathcal{P}, \Delta\mathcal{Z})$ with $Q^2(\mathcal{P}, \langle\Delta\mathcal{Z}\rangle)$ (to be constructed).

Construction

A) $|\Delta\mathcal{Z}| \leq 2$: See next slides.

B) If $|\Delta\mathcal{Z}| \geq 3$:

1. Partition $\Delta\mathcal{Z}$ into $\Delta\mathcal{Z}_1, \Delta\mathcal{Z}_2, \Delta\mathcal{Z}_3$ of similar size.
2. Construct MPC protocols $\bar{\pi}_i$ for each $\Delta\mathcal{Z}_i^c = \Delta\mathcal{Z} \setminus \Delta\mathcal{Z}_i$.
3. Let $\bar{\pi}_1, \bar{\pi}_2, \bar{\pi}_3$ run threshold MPC with $n = 3$, $t = 1$.

Analysis

- Every $Z \in \Delta^{\!*}\mathcal{Z}$ is contained in two $\Delta^{\!*}\mathcal{Z}_i^c$ → honest majority.
- Efficiency: Exp(recursion depth) = Exp(log($|\Delta\mathcal{Z}|$)) = Poly($|\Delta\mathcal{Z}|$).

MPC for Delta Structures (cont'd)

Adding one Adversary Set

- Given: $\bar{\pi}$ for $\mathcal{P}, \mathcal{Z}$ (with $Q^2(\mathcal{P}, \mathcal{Z})$), and an additional set $Z_1 \subseteq \mathcal{P}$.
- Goal: Construct $\bar{\pi}'$ for $\mathcal{P}, (\mathcal{Z} \cup_! \{Z_1\})$.

Construction

$\boxed{Z_1 \text{ is sufficient}}$

1. $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$, $k = |Z_1^c|$ (#honest parties in Z_1).
2. Let $\bar{\pi}' = \bar{\pi}$, where each $P_i \in \mathcal{P}$ is simulated by a threshold protocol among
   $\mathcal{P}_i = \underbrace{Z_1^c}_{k \text{ parties}} \cup \underbrace{\{P_i^1, \ldots, P_i^{k-1}\}}_{k-1 \text{ copies of } P_i}$, tolerating $k-1$ corruptions.

Lemma: The above construction is secure against $(\mathcal{Z} \cup_! \{Z_1\})$

Proof: Consider $Z \in (\mathcal{Z} \cup_! \{Z_1\})$:

A) $Z \in \mathcal{Z}, Z \cup Z_1 \neq \mathcal{P}$: The simulations of honest P_i's have honest majority.

B) $Z = Z_1$: *All* $P_i \in Z$ are correctly simulated!

Efficiency: Poly(n) blow-up for one additional set Z_1.

MPC for Delta Structures (cont'ed)

Adding multiple Adversary Set

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

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

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?