Efficient General-Adversary Multi-Party Computation

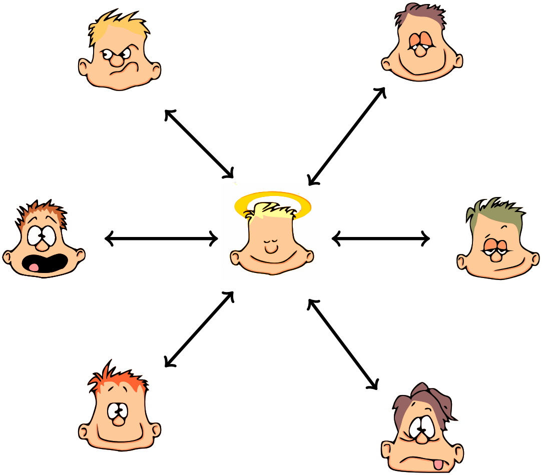
Martin Hirt, **Daniel Tschudi**

ETH Zurich

Dec 2013

Multi-Party Computation

Ideal world: n players, $\mathcal{P} = \{P_1, \ldots, P_n\}$

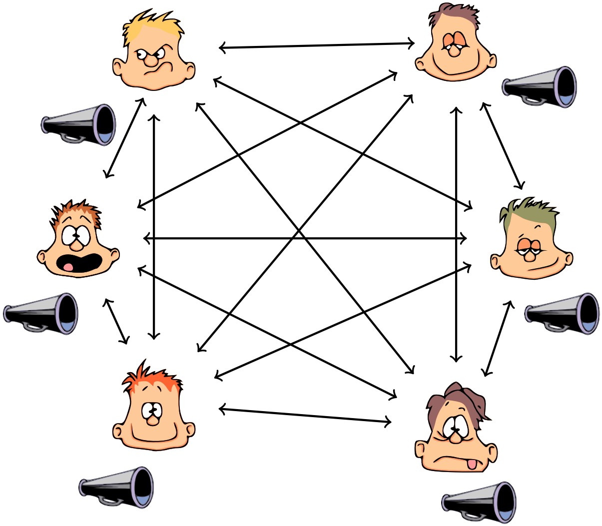


Multi-Party Computation

Reality: n players, $\mathcal{P} = \{P_1, \ldots, P_n\}$

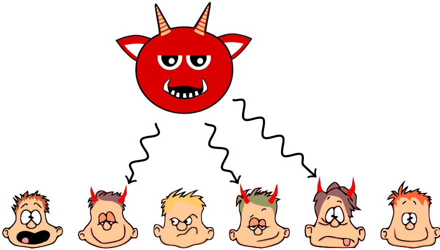
Multi-Party Computation

The Model: secure channels (with broadcast)



The Adversary

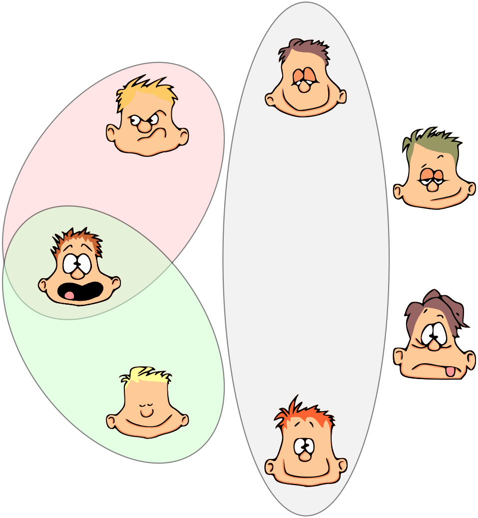
- unbounded central adversary
- corrupts players
- passive/active



Example

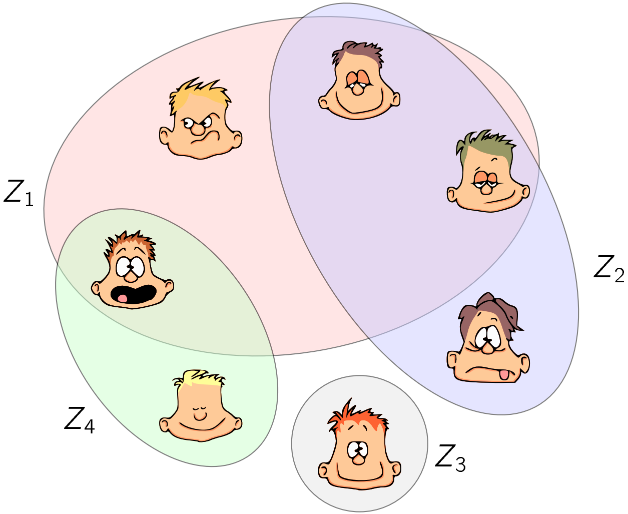
Threshold adversary:
e.g. strictly less then $\frac{n}{3}$ corrupted players

Threshold Adversary

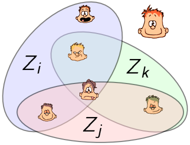


General Adversary

adversary structure $\mathcal{Z} = \{Z_1, \ldots, Z_{|\mathcal{Z}|}\}$



General Adversary



Conditions on the adversary structure $\mathcal{Z}$:

- $\mathcal{Q}^2(\mathcal{P},\mathcal{Z}) :\Longleftrightarrow \mathcal{P} \neq Z_i \cup Z_j \quad \forall Z_i, Z_j \in \mathcal{Z}$
- $\mathcal{Q}^3(\mathcal{P},\mathcal{Z}) :\Longleftrightarrow \mathcal{P} \neq Z_i \cup Z_j \cup Z_k \quad \forall Z_i, Z_j, Z_k \in \mathcal{Z}$

Theorem ([HM97])

$\mathcal{Z}$-secure MPC is possible iff

perfect security: *$\mathcal{Z}$ satisfies $\mathcal{Q}^3$.*

unconditional security: *$\mathcal{Z}$ satisfies $\mathcal{Q}^2$.*

Communication Complexity

- communication is expensive!
- known MPC protocols require $|\mathcal{Z}|^{\mathcal{O}(1)}$ bits of communication.
- near threshold, $\mathcal{Q}^3$: $|\mathcal{Z}| \approx \binom{n}{n/3}$

Example

$n = 30 \Rightarrow |\mathcal{Z}| \approx 30'000'000$:

Complexity	$\lvert\mathcal{Z}\rvert$	$\lvert\mathcal{Z}\rvert^2$	$\lvert\mathcal{Z}\rvert^3$
Runtime	1 second	347 days	30 million years

Efficient protocols have a small exponent!

Communication Complexity

Setting	Cond.	Bits / Mult.	Reference
passive perfect	$\mathcal{Q}^2$	$\lvert\mathcal{Z}\rvert \cdot \mathrm{Poly}(n)$	[Mau02]
active perfect	$\mathcal{Q}^3$	$\lvert\mathcal{Z}\rvert^3 \cdot \mathrm{Poly}(n)$	[Mau02]
active perfect	$\mathcal{Q}^3$	$\lvert\mathcal{Z}\rvert^2 \cdot \mathrm{Poly}(n)$	our result
active uncond.	$\mathcal{Q}^2$	$\lvert\mathcal{Z}\rvert^3 \cdot \mathrm{Poly}(n, \kappa)$	[Mau02]/[BFH+08]
active uncond.	$\mathcal{Q}^3$	$\lvert\mathcal{Z}\rvert^2 \cdot \mathrm{Poly}(n, \kappa)$	[PSR03]
active uncond.	$\mathcal{Q}^2$	$\lvert\mathcal{Z}\rvert \cdot \mathrm{Poly}(n, \kappa)$	our result

The Computation

Specified by a circuit over finite field $\mathbb{F}$:

- Input and output gates
- Addition gates
- Multiplication gates

Verifiable Secret Sharing (VSS)

Z_1		a_1		a_1	a_1
Z_2		a_2	a_2		a_2
Z_3	a_3		a_3	a_3	a_3
$\vdots$					
$Z_{\lvert\mathcal{Z}\rvert}$		$a_{\lvert\mathcal{Z}\rvert}$	$a_{\lvert\mathcal{Z}\rvert}$	$a_{\lvert\mathcal{Z}\rvert}$	

$$a = a_1 + a_2 + a_3 + \vdots + a_{|\mathcal{Z}|}$$

Verifiable Secret Sharing (VSS)

Z_1		$a_1 + b_1$		$a_1 + b_1$	$a_1 + b_1$
Z_2		$a_2 + b_2$	$a_2 + b_2$		$a_2 + b_2$
Z_3	$a_3 + b_3$		$a_3 + b_3$	$a_3 + b_3$	$a_3 + b_3$
$\vdots$					
$Z_{\vert\mathcal{Z}\vert}$		$a_{\vert\mathcal{Z}\vert}+b_{\vert\mathcal{Z}\vert}$	$a_{\vert\mathcal{Z}\vert}+b_{\vert\mathcal{Z}\vert}$	$a_{\vert\mathcal{Z}\vert}+b_{\vert\mathcal{Z}\vert}$	

$$a + b = a_1 + b_1 + a_2 + b_2 + a_3 + b_3 + \vdots + a_{|\mathcal{Z}|} + b_{|\mathcal{Z}|}$$

Linearity!

Verifiable Secret Sharing (VSS)

Let $S_i := Z_i^c$

A value s is shared if

- s split in random summands $s_1, \ldots, s_{|\mathcal{Z}|}$
- $\forall P \in S_i$ knows s_i.

Denote a shared s by $[s]$.

Protocols: [Mau02]

- Share
- Reconstruct

Both protocols have complexity $|\mathcal{Z}| \cdot \mathrm{Poly}(n)$

The Computation

Specified by a circuit over finite field $\mathbb{F}$:

- Input and output gates: Share / Reconstruct $|\mathcal{Z}| \cdot \mathrm{Poly}(n)$
- Addition gates: linearity of VSS for free!
- Multiplication gates of shared values:

$$a = a_1 + \cdots + a_{|\mathcal{Z}|}, \quad b = b_1 + \cdots + b_{|\mathcal{Z}|}$$

$$ab = \sum_{i=1}^{|\mathcal{Z}|} a_i \sum_{j=1}^{|\mathcal{Z}|} b_j = \sum_{i=1}^{|\mathcal{Z}|} \sum_{j=1}^{|\mathcal{Z}|} (a_i b_j)$$

Passive Multiplication

Multiplication([a], [b]) [Mau02]

For each (i, j) do $|\mathcal{Z}|^2$ products

- Some $P_k \in S_i \cap S_j$ shares $a_i b_j$ as $[v_{ij}]$ $|\mathcal{Z}| \cdot \mathrm{Poly}(n)$

end

for free

Complexity: $|\mathcal{Z}|^3 \cdot \mathrm{Poly}(n)$

Passive Multiplication

Multiplication($[a]$, $[b]$) [Mau02]

For each (i, j) do — $|\mathcal{Z}|^2$ products

- Some $P_k \in S_i \cap S_j$ shares $a_i b_j$ as $[v_{ij}]$ — $|\mathcal{Z}| \cdot \mathrm{Poly}(n)$

end

$$[ab] = \sum_{i,j=1}^{|\mathcal{Z}|} [v_{ij}]$$ for free

Complexity: $|\mathcal{Z}| \cdot \mathrm{Poly}(n)$

Optimization:
Each P_k shares $\sum_{(i,j) \in L_k} v_{ij}$

Active Multiplication

Multiplication([a], [b]) [Mau02]

For each (i,j) do — $|\mathcal{Z}|^2$ products

- Every $P_k \in S_i \cap S_j$ share $a_i b_j$ as $[v_{ij}^k]$ — $|\mathcal{Z}| \cdot \text{Poly}(n)$

end

$$[ab] = \sum_{i,j=1}^{|\mathcal{Z}|} [v_{ij}^1]$$

Check: $[v_{ij}^1] - [v_{ij}^k] \stackrel{?}{=} 0 \ \forall P_k$ — for free

Complexity: $|\mathcal{Z}|^3 \cdot \text{Poly}(n)$

Optimistic Active Multiplication

Assume Z_k is the adversary set:

Optimistic Multiplication($[a], [b], Z_k$)

For each (i, j) do $\quad |\mathcal{Z}|^2$ products

- Some $P_k \in S_i \cap S_j \setminus Z_k$ shares $a_i b_j$ as $[v_{ij}]$ $\quad |\mathcal{Z}| \cdot \text{Poly}(n)$

end

$$[ab] = \sum_{i,j=1}^{|\mathcal{Z}|} [v_{ij}]$$

for free

Protocol secure against Z_k!

Complexity: $|\mathcal{Z}|^3 \cdot \text{Poly}(n)$

Optimistic Active Multiplication

Assume Z_k is the adversary set:

Optimistic Multiplication($[a], [b], Z_k$)

For each (i, j) do $|\mathcal{Z}|^2$ products

- Some $P_k \in S_i \cap S_j \setminus Z_k$ shares $a_i b_j$ as $[v_{ij}]$ $|\mathcal{Z}| \cdot \mathrm{Poly}(n)$

end

$$[ab] = \sum_{i,j=1}^{|\mathcal{Z}|} [v_{ij}]$$

for free

Complexity: $|\mathcal{Z}| \cdot \mathrm{Poly}(n)$

Optimization:
Each P_k shares $\sum_{(i,j) \in L_k} v_{ij}$

Efficient Multiplication

Multiplication([a], [b])

For each $Z_k \in Z$ do — $|\mathcal{Z}|$ sets

- $[c_k] :=$ Optimistic Multiplication$([a],[b],Z_k)$. — $|\mathcal{Z}| \cdot \text{Poly}(n)$

end

Check: $[c_1] - [c_k] \stackrel{?}{=} 0 \ \ \forall k$ — $|\mathcal{Z}|^2 \cdot \text{Poly}(n)$

If yes $[ab] := [c_1]$, otherwise eliminate a cheater and repeat!

Complexity: $|\mathcal{Z}|^2 \cdot \text{Poly}(n)$

At most n times!

The Computation

Specified by a circuit over finite field $\mathbb{F}$:

- Input and output gates: Share / Reconstruct $|\mathcal{Z}| \cdot \text{Poly}(n)$
- Addition gates: linearity of VSS for free!
- Multiplication gates : Optimistic Multiplication $|\mathcal{Z}|^2 \cdot \text{Poly}(n)$

Unconditional protocol:

- Sharing with Information Checking ($\mathcal{Q}^2$)
- Optimistic Multiplication with probabilistic checks
- Bits per multiplication: $|\mathcal{Z}| \cdot \mathsf{Poly}(n, \kappa)$

Conclusion

Setting	Cond.	Bits / Mult.	Reference
passive perfect	$\mathcal{Q}^2$	$\lvert\mathcal{Z}\rvert \cdot \mathrm{Poly}(n)$	[Mau02]
active perfect	$\mathcal{Q}^3$	$\lvert\mathcal{Z}\rvert^3 \cdot \mathrm{Poly}(n)$	[Mau02]
active perfect	$\mathcal{Q}^3$	$\lvert\mathcal{Z}\rvert^2 \cdot \mathrm{Poly}(n)$	our result
active uncond.	$\mathcal{Q}^2$	$\lvert\mathcal{Z}\rvert^3 \cdot \mathrm{Poly}(n, \kappa)$	[Mau02]/[BFH+08]
active uncond.	$\mathcal{Q}^3$	$\lvert\mathcal{Z}\rvert^2 \cdot \mathrm{Poly}(n, \kappa)$	[PSR03]
active uncond.	$\mathcal{Q}^2$	$\lvert\mathcal{Z}\rvert \cdot \mathrm{Poly}(n, \kappa)$	our result

Precise bounds
see paper!