Layered MPC

Perfect MPC over Layered Graphs

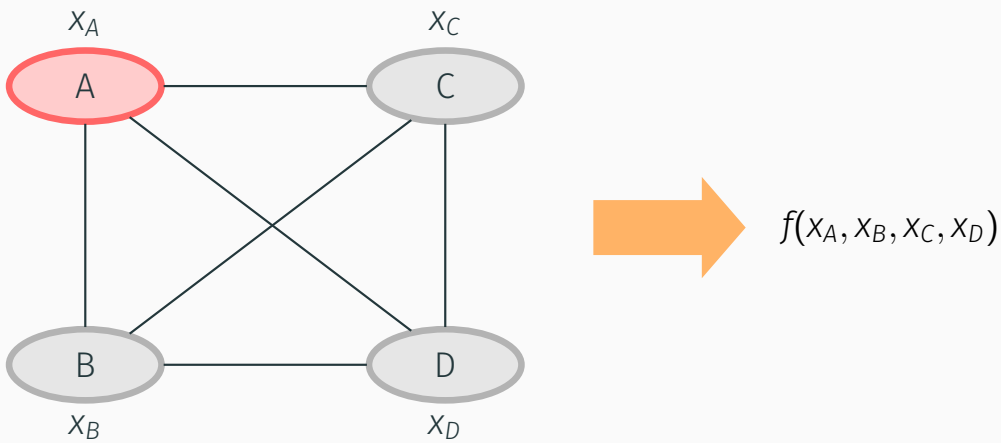
Bernardo David, Anders Konring IT University of Copenhagen
Yuval Ishai, Eyal Kushilevitz Technion - Israel Institute of Technology
Varun Narayanan UCLA
Aarushi Goel NTT Research - US
Chen-Da Liu-Zhang Web3 Foundation and HSLU
Giovanni Deligios ETH Zurich

Table of contents

Motivation

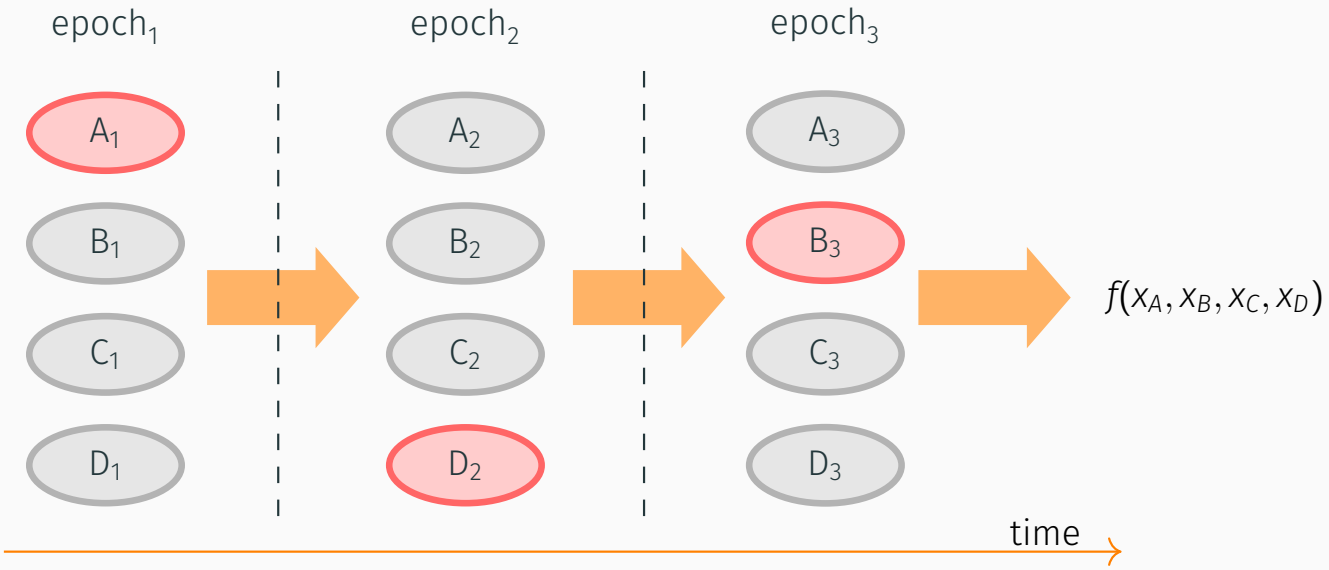
Brief History

- [BGW88]: general MPC with perfect, full security and optimal threshold ($t < n/3$).



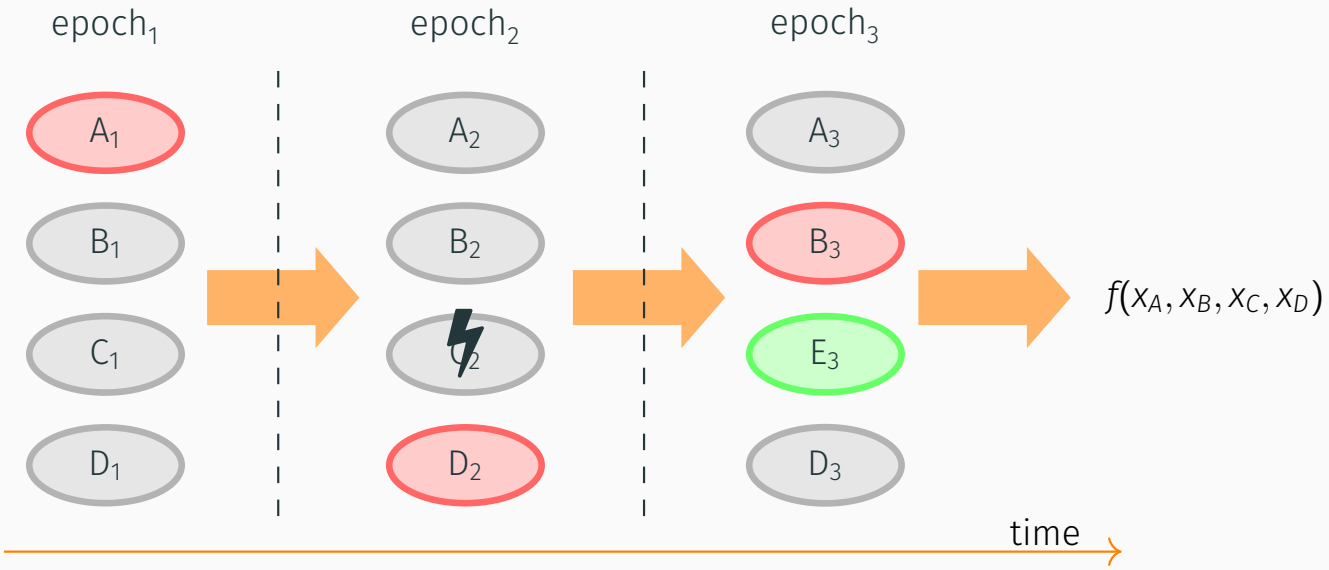
Brief History

- [BGW88]: general MPC with perfect, full security and optimal threshold ($t < n/3$).
- [OY91]: feasibility result of general MPC with **mobile adversary**
  - Show feasibility of general IT MPC [BGW88, RB89].
- [HJKY95, BELO14, CH01]: **Proactive** Secret Sharing & MPC.



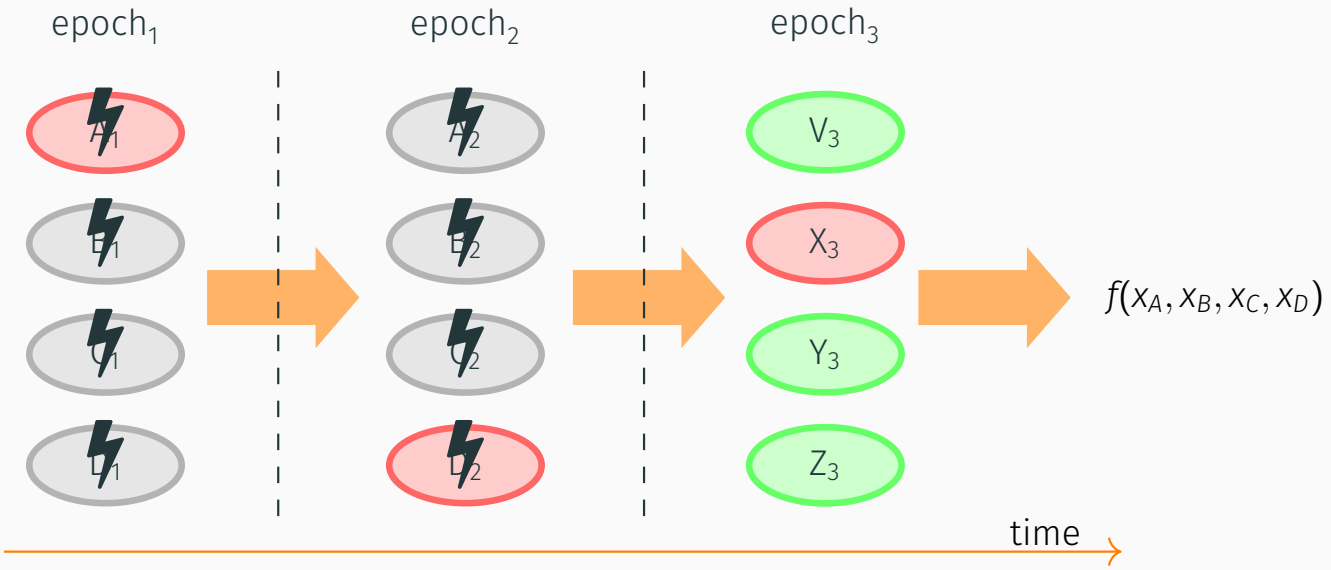
Brief History

- [BGW88]: general MPC with perfect, full security and optimal threshold ($t < n/3$).
- [OY91]: feasibility result of general MPC with **mobile adversary**
  - Show feasibility of general IT MPC [BGW88, RB89].
- [HJKY95, BELO14, CH01]: **Proactive** Secret Sharing & MPC.
- [DJ97, WWW02, MZW+19, ELL20]: **Dynamic Proactive** SS & MPC.

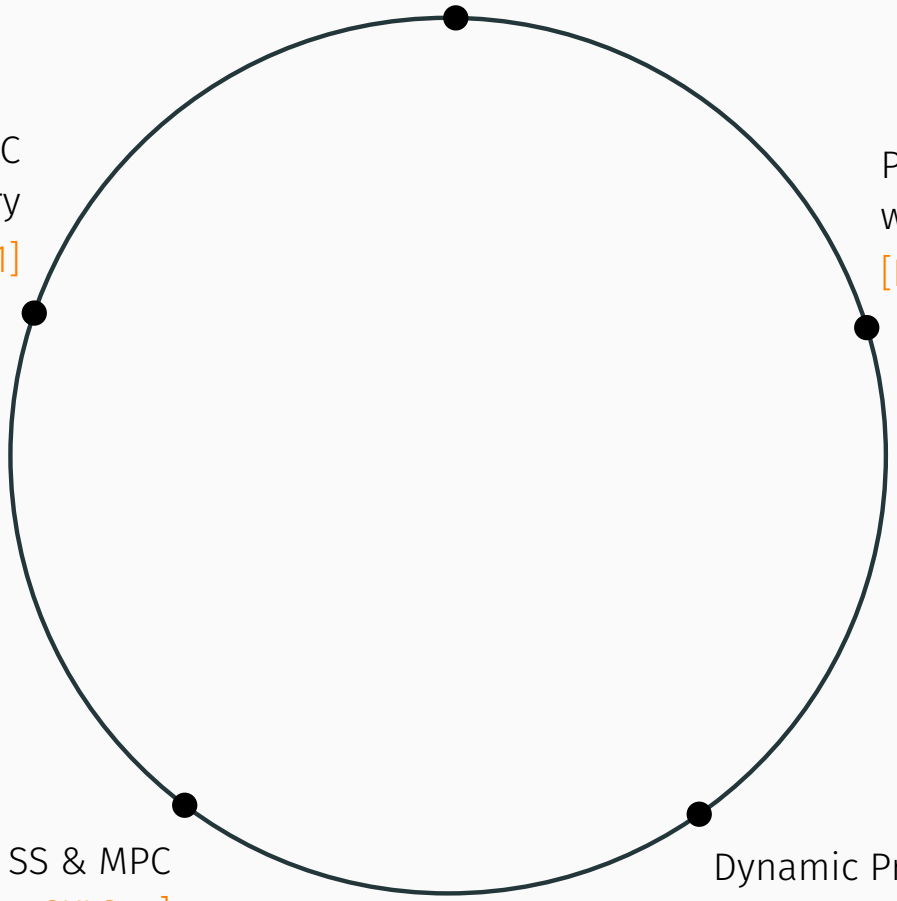


Brief History

- [BGW88]: general MPC with perfect, full security and optimal threshold ($t < n/3$).
- [OY91]: feasibility result of general MPC with **mobile adversary**
  - Show feasibility of general IT MPC [BGW88, RB89].
- [HJKY95, BELO14, CH01]: **Proactive** Secret Sharing & MPC.
- [DJ97, WWW02, MZW+19, ELL20]: **Dynamic Proactive** SS & MPC.
- [GHM+17, BGG+20, GHK+21, CGG+21]: Secret sharing and MPC using **ephemeral committees** (YOSO, Fluid).



Brief History



Perfect General MPC, $t < n/3$
[BGW88]

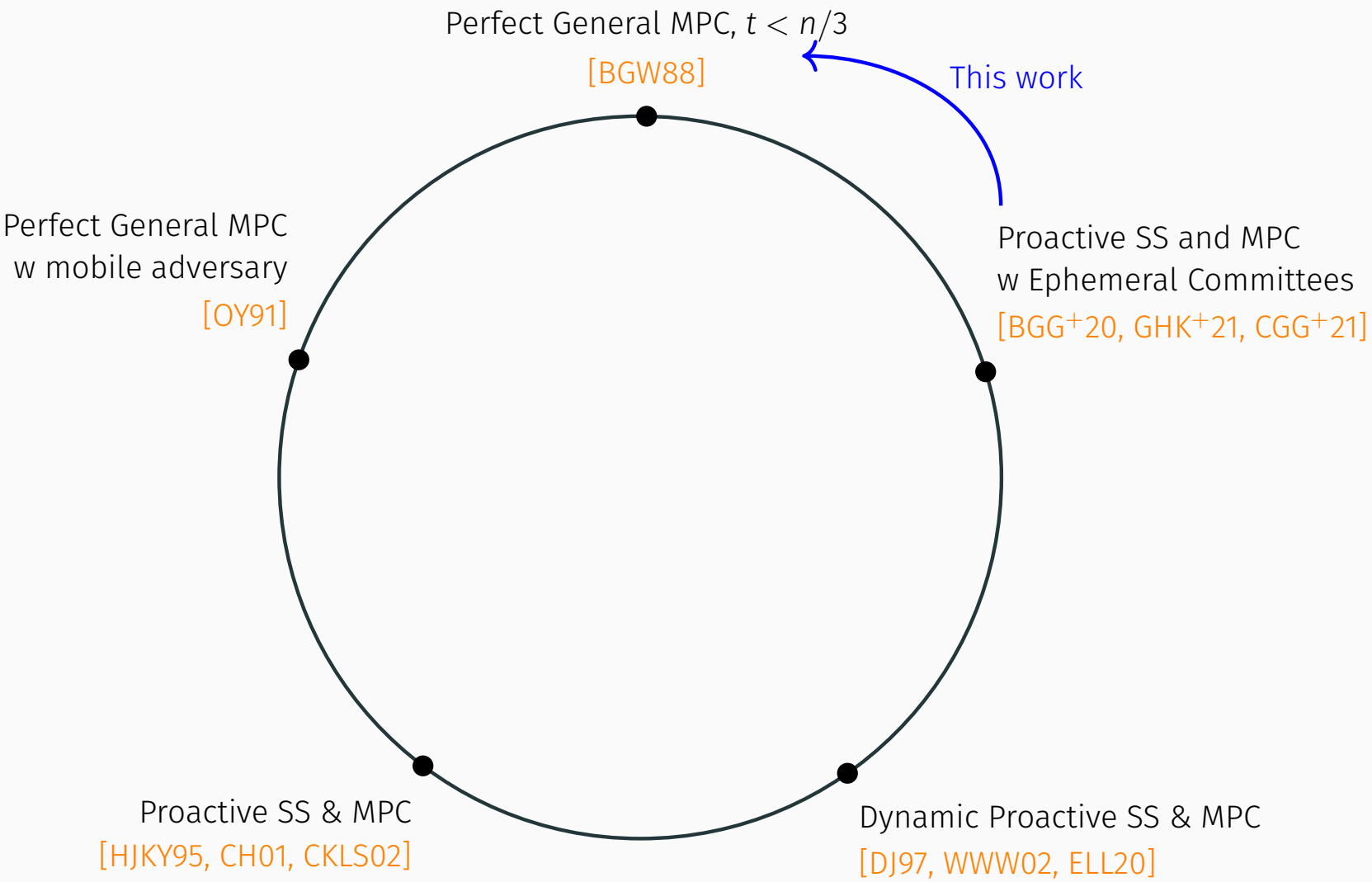
Proactive SS and MPC
w Ephemeral Committees
[BGG+20, GHK+21, CGG+21]

Dynamic Proactive SS & MPC
[DJ97, WWW02, ELL20]

Proactive SS & MPC
[HJKY95, CH01, CKLS02]

Perfect General MPC
w mobile adversary
[OY91]

Brief History



Motivation

Is it possible to construct MPC with **ephemeral committees** *achieving* **perfect full security** *against a* **maximally mobile adversary*** *while maintaining* **optimal corruption threshold***?*

*An epoch contains a single round, $|\text{epoch}| = 1$

Contributions

Area	Reference	|epoch|	Security	Corruption	Setup (BC+Chan.)
Proactive MPC	[HJKY95]	>1	Comp (full)	$t < n/2$	Next Round
	[OY91]	=1	Stat (full)	$t < n/c$[†]	Next Round
Ephemeral Committees	[GHK+21] (YOSO)	=1	Stat (full)	$\mathbb{E}[t] < n/2$	Any Future Round
	[CGG+21] (Fluid)	=1	Stat (abort)	$t < n/2$	Next Round

[†]The adversary may corrupt at most a constant fraction of parties.

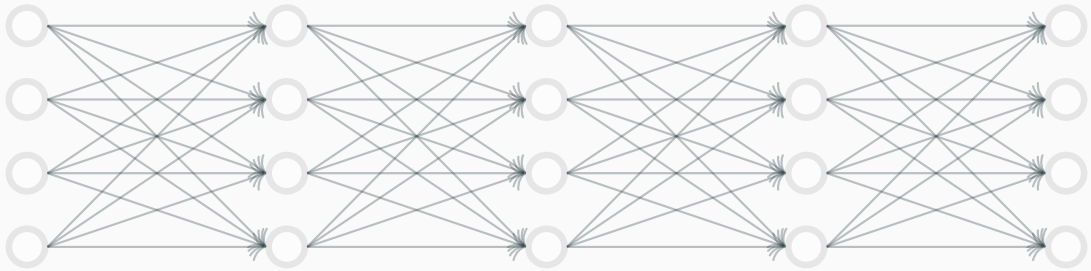
Contributions

Area	Reference	|epoch|	Security	Corruption	Setup (BC+Chan.)
Proactive MPC	[HJKY95]	>1	Comp (full)	$t < n/2$	Next Round
	[OY91]	=1	Stat (full)	$t < n/c^{\dagger}$	Next Round
Ephemeral Committees	[GHK+21] (YOSO)	=1	Stat (full)	$\mathbb{E}[t] < n/2$	Any Future Round
	[CGG+21] (Fluid)	=1	Stat (abort)	$t < n/2$	Next Round
	This work	=1	Perfect (full)	$t < n/3$	Next Round

[†]The adversary may corrupt at most a constant fraction of parties.

Contributions

Layered MPC is an instance of standard MPC [Can00, Gol09, HM00] with restricted interaction pattern [HIJ+16] induced by a graph G.



Use the setting of layered MPC to (indirectly) study protocols for maximally proactive MPC [OY91].

Lemma 1

Secure Layered MPC $\Rightarrow^*$ Secure Maximally Proactive MPC

* assuming secure erasures

Contributions

Main Contribution:

- Formalize the model of **Layered MPC**—standard MPC with special interaction pattern and adversary structure.

Contributions

Main Contribution:

- Formalize the model of **Layered MPC**—standard MPC with special interaction pattern and adversary structure.
- Present layered MPC protocols for general functionalities with **perfect, full security** and **optimal corruption threshold** $t < n/3$.
  - CNF (Replicated) Secret Sharing based protocols [GIKR01, Mau06].
  - Shamir Secret Sharing based protocols (efficient) [BGW88].

Contributions

Main Contribution:

- Formalize the model of **Layered MPC**—standard MPC with special interaction pattern and adversary structure.
- Present layered MPC protocols for general functionalities with **perfect, full security** and **optimal corruption threshold** $t < n/3$.
  - CNF (Replicated) Secret Sharing based protocols [GIKR01, Mau06].
  - Shamir Secret Sharing based protocols (efficient) [BGW88].
- Improve on existing results on **maximally proactive** MPC protocols [OY91] and on new work on MPC with **ephemeral committees** [GHK+21, CGG+21].

Contributions

Main Contribution:

- Formalize the model of **Layered MPC**—standard MPC with special interaction pattern and adversary structure.
- Present layered MPC protocols for general functionalities with **perfect, full security** and **optimal corruption threshold** $t < n/3$.
  - CNF (Replicated) Secret Sharing based protocols [GIKR01, Mau06].
  - Shamir Secret Sharing based protocols (efficient) [BGW88].
- Improve on existing results on **maximally proactive** MPC protocols [OY91] and on new work on MPC with **ephemeral committees** [GHK+21, CGG+21].
- Present layered MPC protocols for general functionalities with **computational, full security** and $t < n/2$.

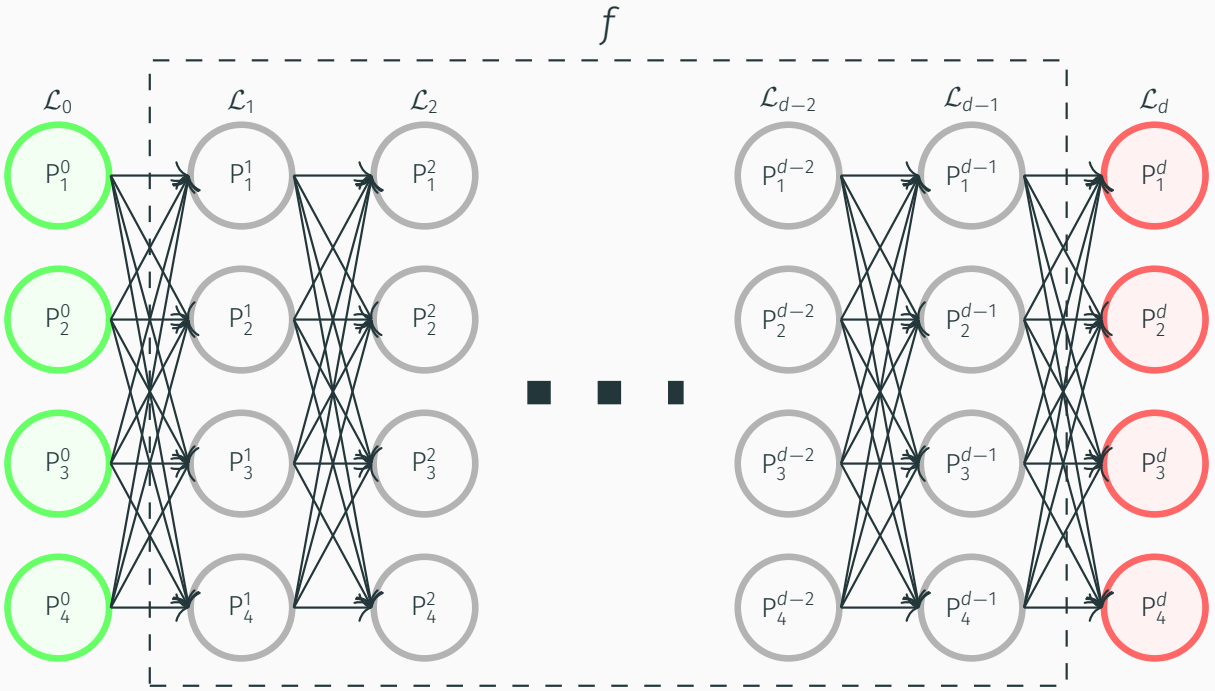
Layered MPC

Layered MPC

An (n, t, d)-**layered protocol** has the following properties:

Parties. $N = n(d+1)$ parties partitioned into $d+1$ layers $\mathcal{L}_i$, $0 \leq i \leq d$, where $|\mathcal{L}_i| = n$.

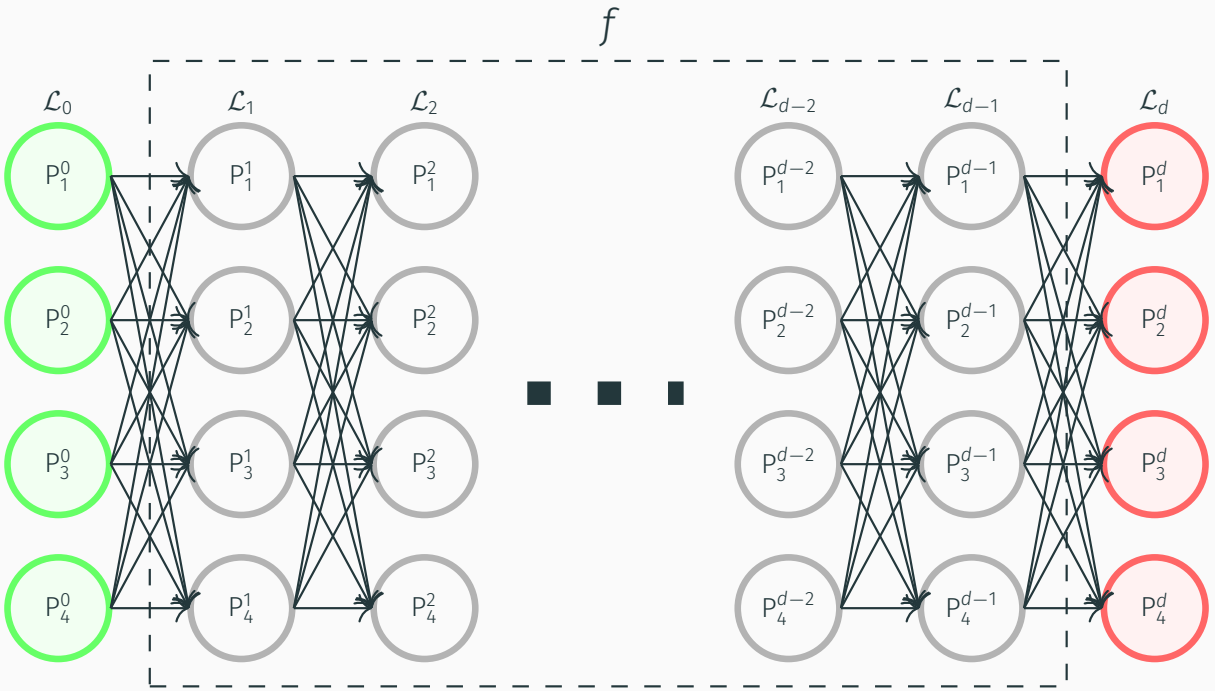
Interaction. d synchronous rounds where parties in $\mathcal{L}_{i-1}$ may send messages to parties in $\mathcal{L}_i$ over secure channels and broadcast.



Layered MPC

Functionalities. We consider functionalities f that take inputs from input clients and deliver outputs to output clients.

Adversaries. We consider active, rushing, adaptive adversaries who may corrupt any number of input/output clients, and t parties in layers $\mathcal{L}_i$, $0 < i < d$.



Layered MPC

A note on Layered Broadcast

- The model of layered MPC assumes layer-to-layer broadcast.
- Deterministic Broadcast is impossible in the layered setting.
- Derived from the result of [Gar94] on reaching agreement in the mobile setting.

Lemma 2

Deterministic Broadcast is possible iff $t = 0$.

Basic Primitives

Future Messaging

Future Messaging functionality f_{FM}

PUBLIC PARAMETERS: Sender $\mathsf{S} \in \mathcal{L}_0$, receiver $\mathsf{R} \in \mathcal{L}_d$ for $d > 0$ and message domain M.

SECRET INPUTS: S has input $m \in M$.

f_{FM} receives m from S, and delivers m to R.

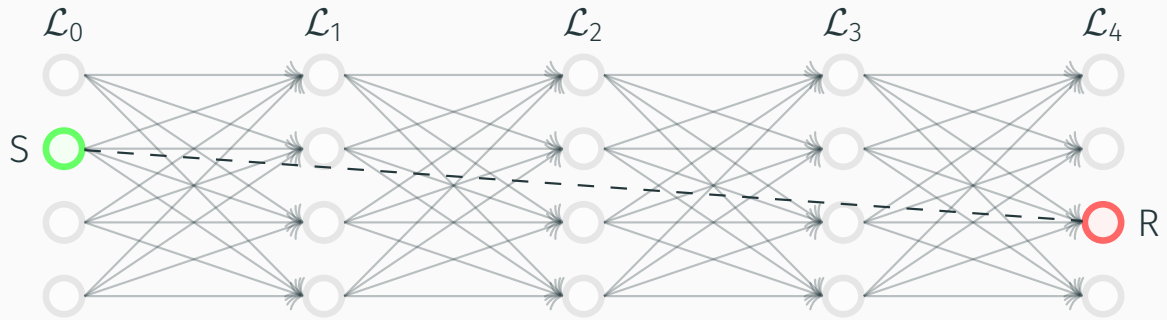
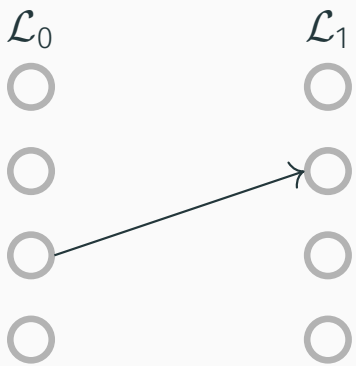


Figure 1: Π_{FM} from S of m to R

Future Messaging

Π_{FM} from $\mathcal{L}_0$ to $\mathcal{L}_1$:

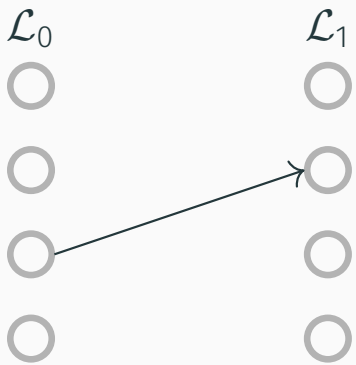
Use the secure point-to-point channels from layer to the next layer.



Future Messaging

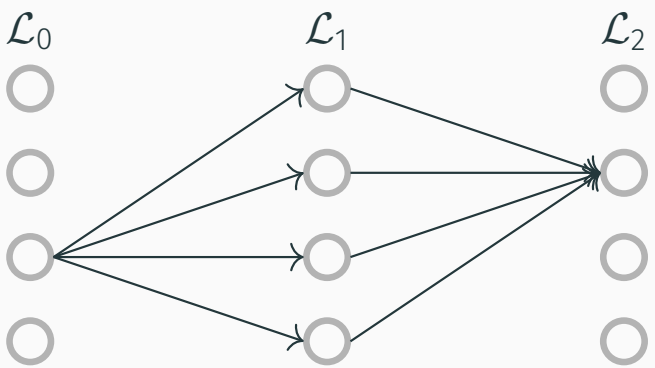
Π_{FM} from $\mathcal{L}_0$ to $\mathcal{L}_1$:

Use the secure point-to-point channels from layer to the next layer.



Π_{FM} from $\mathcal{L}_0$ to $\mathcal{L}_2$:

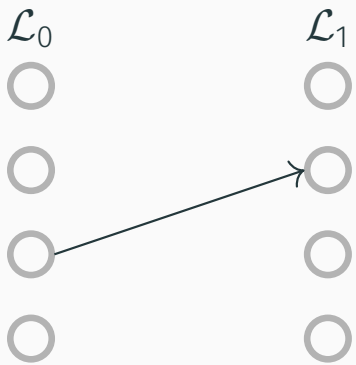
1. S does $\mathrm{Sh}(m) = (s_1, \ldots, s_n)$ and sends s_j to P_j^1.
2. P_j^1 forwards s_j to R and R obtains $\hat{m} = \mathrm{Rec}(\hat{s}_1, \ldots, \hat{s}_n)$



Future Messaging

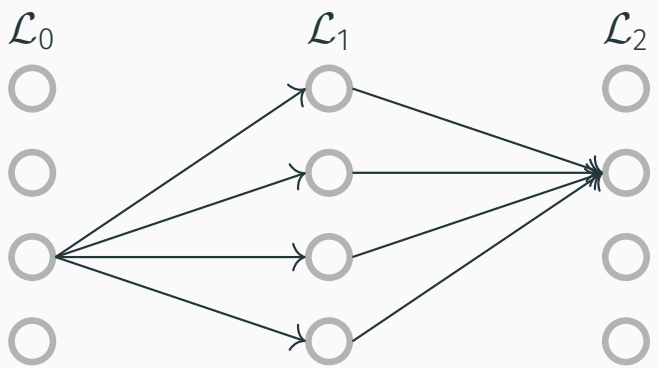
Π_{FM} from $\mathcal{L}_0$ to $\mathcal{L}_1$:

Use the secure point-to-point channels from layer to the next layer.



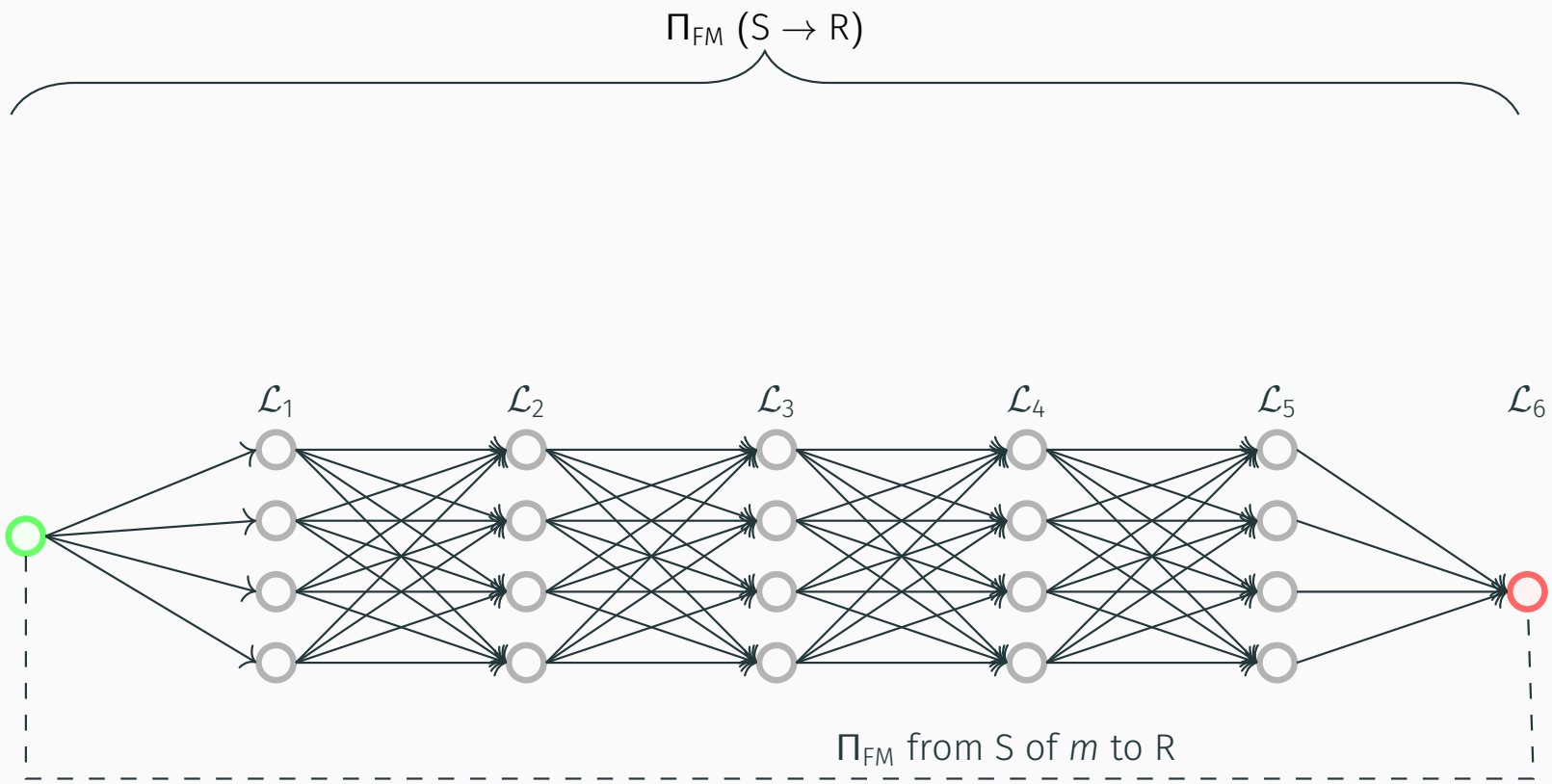
Π_{FM} from $\mathcal{L}_0$ to $\mathcal{L}_2$:

1. S does $\mathsf{Sh}(m) = (s_1, \ldots, s_n)$ and sends s_j to P_j^1.
2. P_j^1 forwards s_j to R and R obtains $\hat{m} = \mathsf{Rec}(\hat{s}_1, \ldots, \hat{s}_n)$

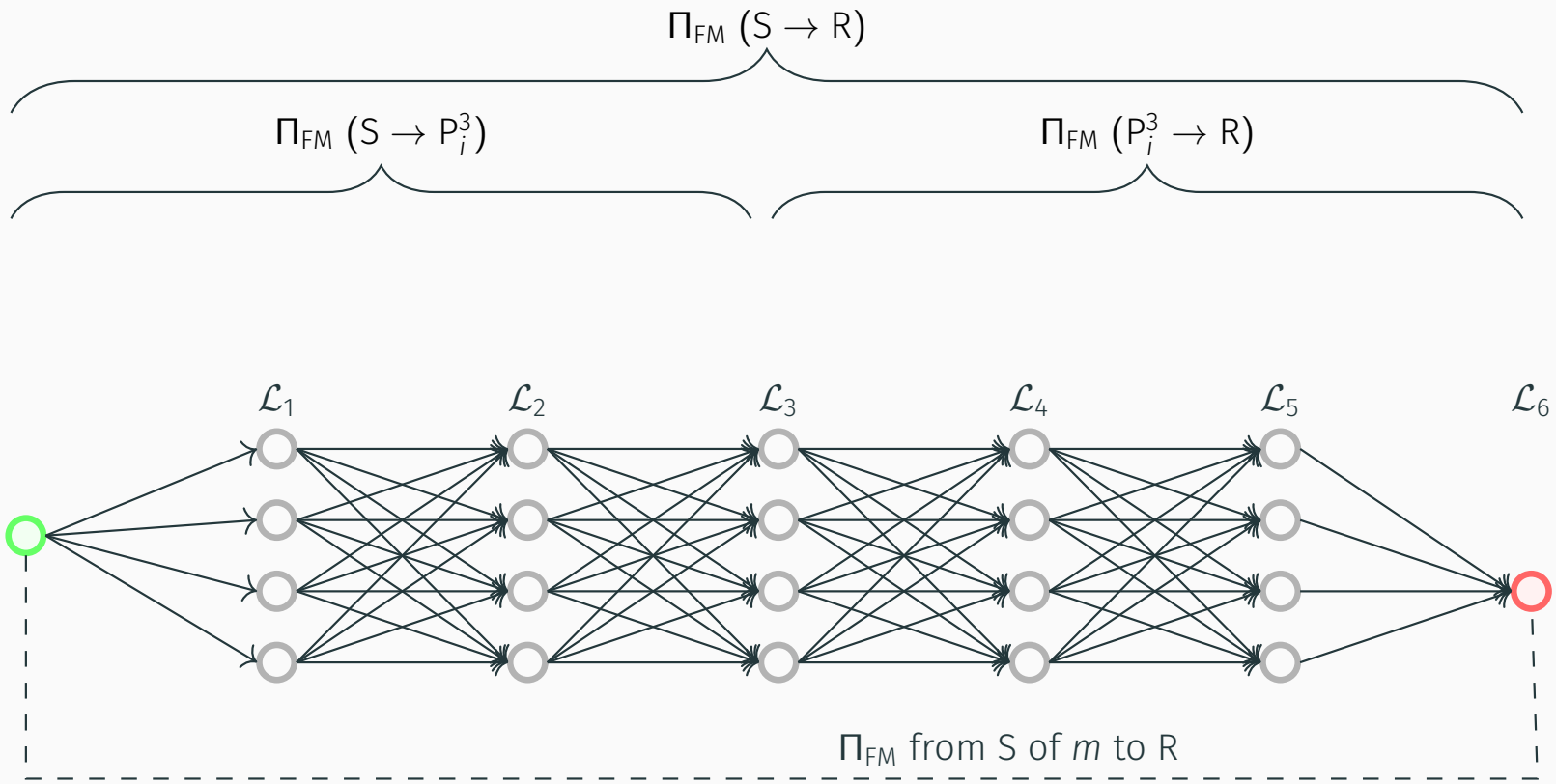


(Equivalent to perfect malicious 1-way SMT [DDWY93])

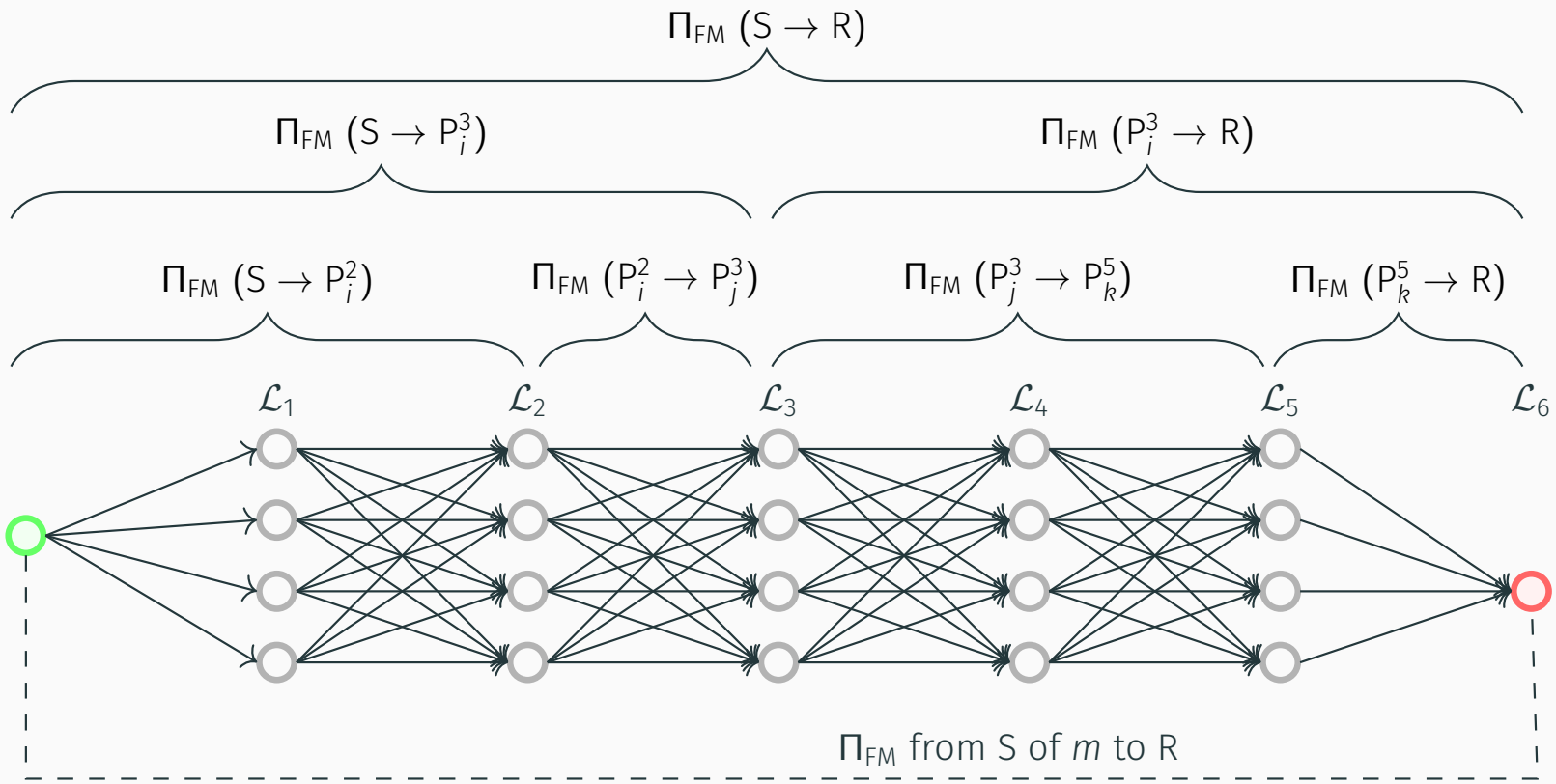
Future Messaging



Future Messaging



Future Messaging

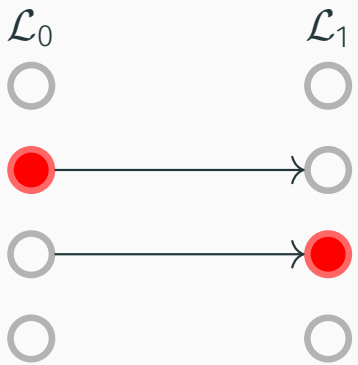


Future Messaging (and Rushing)

Dishonest Sender and problems with rushing

Parallel Invocations f_{FM}^{n}:

- When invoking multiple f_{FM} in parallel, the adversary can cause a **correlation attack**.
- Model the parallel functionality as **corruption-aware**.

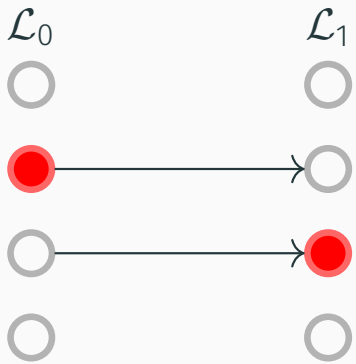


Future Messaging (and Rushing)

Dishonest Sender and problems with rushing

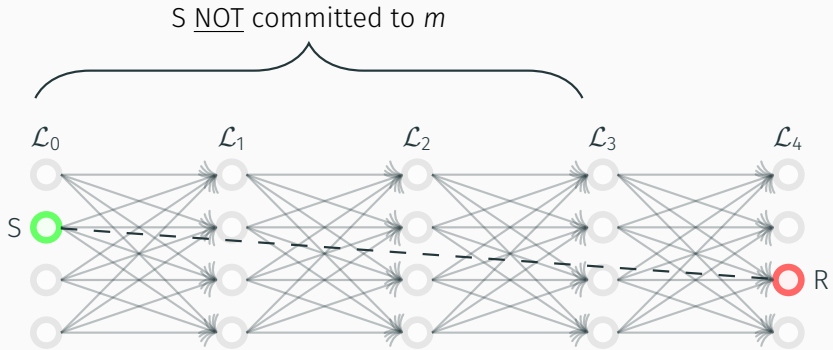
Parallel Invocations f_{FM}^{n}:

- When invoking multiple f_{FM} in parallel, the adversary can cause a **correlation attack**.
- Model the parallel functionality as **corruption-aware**.



Non-committing Primitive:

- The adversary can change the message m to a message of its choosing m' in f_{FM} until the last round.
- Where YOSO assumes ideal **committing** communication to future rounds.

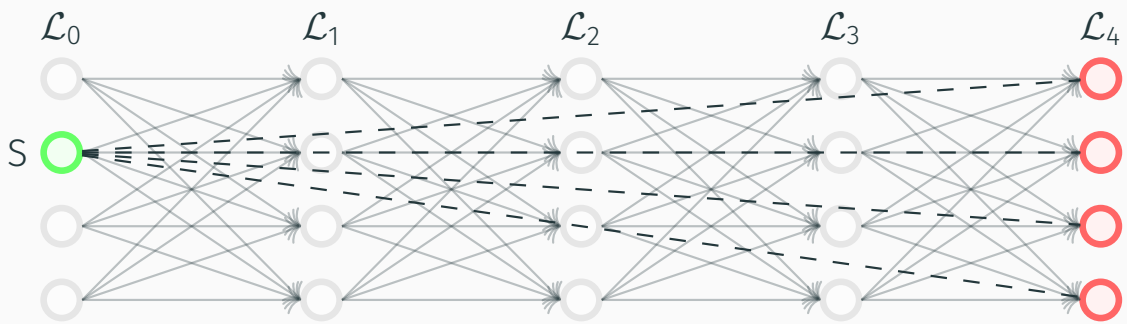


Future Broadcast

(Conditional) Future Broadcast

- Future Broadcast:
  Invoke f_{FM} where parties in $\mathcal{L}_{d-1}$ are instructed to broadcast their shares instead of sending to a recipient R.

- Conditional Disclosure:
  Conditioned on some event E, honest parties in $\mathcal{L}_{d-1}$ reveal their shares.



Future Messaging

Summary of Future Messaging

Complexity Assuming a linear secret sharing scheme, Π_{FM} is a recursive protocol realizing f_{FM} with communication complexity $O(n^{\lceil \log d \rceil} \log |M|)$.

Security Honest sender reduces to an instance of SMT
Dishonest sender is challenging with rushing.
Especially, when composing protocols.

Extension Future Messaging can be extended to (Conditional) Future Broadcast.

Towards Layered MPC

Layered CNF-VSS Protocol

Design Approach

CNF-VSS of [GIKR01]

Weak Future Multicast $\Pi_{\text{weak-FMcast}}$

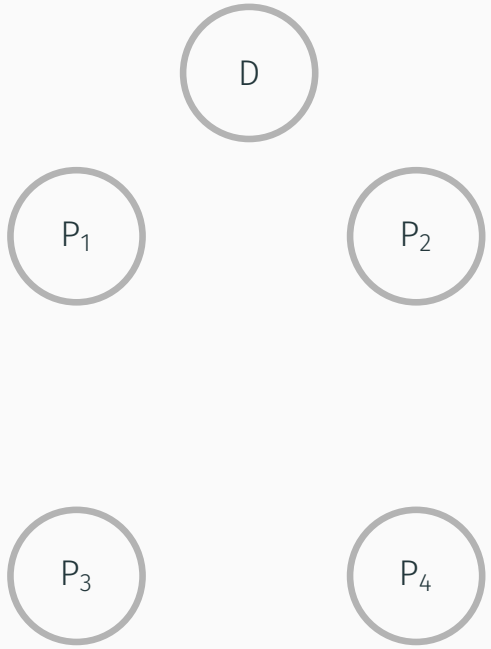
Future Multicast Π_{FMcast}

Verifiable Secret Sharing Π_{VSS}

Techniques from [GIKR01]

4-round perfect CNF VSS

D (dealer) holds a secret $s \in \mathbb{F}$ and obtains $\mathrm{Sh}_{\mathrm{CNF}}(s) = (s_1, \ldots, s_n)$.

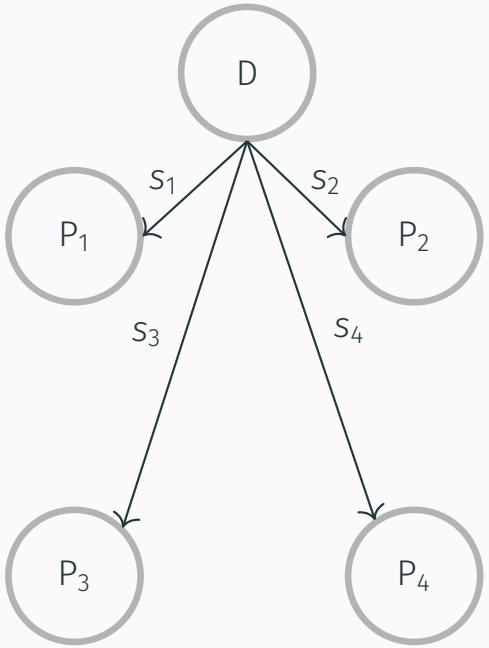


Techniques from [GIKR01]

4-round perfect CNF VSS

D (dealer) holds a secret $s \in \mathbb{F}$ and obtains $\mathrm{Sh}_{\mathrm{CNF}}(s) = (s_1, \ldots, s_n)$.

1. D sends $s_j = (r_T)_{T \ni j}$ to P_j.

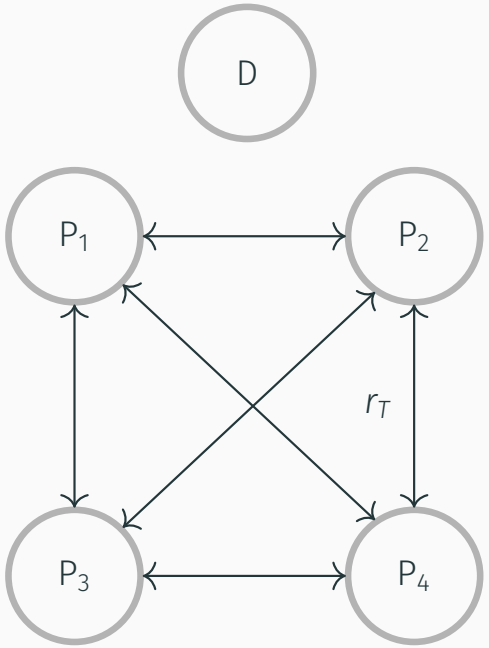


Techniques from [GIKR01]

4-round perfect CNF VSS

D (dealer) holds a secret $s \in \mathbb{F}$ and obtains $\mathrm{Sh}_{\mathrm{CNF}}(s) = (s_1, \ldots, s_n)$.

1. D sends $s_j = (r_T)_{T \ni j}$ to P_j.
2. Each pair $(\mathrm{P}_j, \mathrm{P}_{j'})$ exchange share r_T (if $j, j' \in T$).

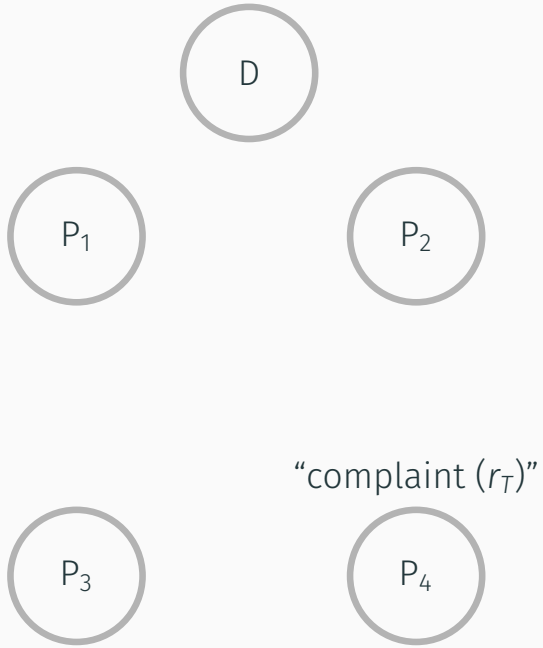


Techniques from [GIKR01]

4-round perfect CNF VSS

D (dealer) holds a secret $s \in \mathbb{F}$ and obtains $\mathrm{Sh}_{\mathrm{CNF}}(s) = (s_1, \ldots, s_n)$.

1. D sends $s_j = (r_T)_{T \ni j}$ to P_j.
2. Each pair $(\mathrm{P}_j, \mathrm{P}_{j'})$ exchange share r_T (if $j, j' \in T$).
3. If disagreement, involved parties broadcast "complaint (r_T)".

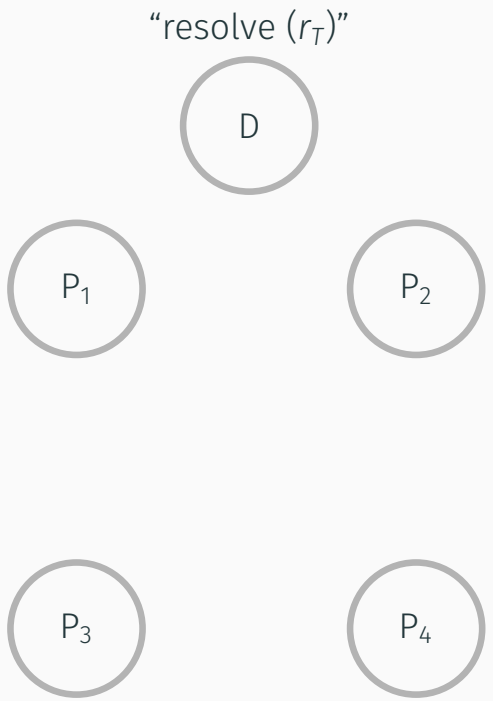


Techniques from [GIKR01]

4-round perfect CNF VSS

D (dealer) holds a secret $s \in \mathbb{F}$ and obtains $\mathrm{Sh}_{\mathrm{CNF}}(s) = (s_1, \ldots, s_n)$.

1. D sends $s_j = (r_T)_{T \ni j}$ to P_j.
2. Each pair $(\mathrm{P}_j, \mathrm{P}_{j'})$ exchange share r_T (if $j, j' \in T$).
3. If disagreement, involved parties broadcast "complaint (r_T)".
4. D then broadcasts "resolve (r_T)", if any complaints received from P_j or $\mathrm{P}_{j'}$.



Techniques from [GIKR01]

Challenges with layered [GIKR01]

- Dealer speaks more than once (round 1 and round 4).

Techniques from [GIKR01]

Challenges with layered [GIKR01]

- Dealer speaks more than once (round 1 and round 4).

  Solution:
  Emulate the dealer using Conditional Future Broadcast.

Techniques from [GIKR01]

Challenges with layered [GIKR01]

- Dealer speaks more than once (round 1 and round 4).

  Solution:
  Emulate the dealer using Conditional Future Broadcast.

- P_j and $P_{j'}$ exchange additive shares.

Techniques from [GIKR01]

Challenges with layered [GIKR01]

- Dealer speaks more than once (round 1 and round 4).

  Solution:
  Emulate the dealer using Conditional Future Broadcast.

- P_j and $P_{j'}$ exchange additive shares.

  Solution:
  Invoke a Distributed Equality Check with Π_{add} for each pair (j, j').

Future Multicast

Future Multicast functionality f_{FMcast}

PUBLIC PARAMETERS: Sender $S \in \mathcal{L}_0$, receiving set of parties $R \subseteq \mathcal{L}_d, d \geq 5$, message domain M.

SECRET INPUTS: S has input $m \in M$.

f_{FMcast} receives m from S, and delivers m to all parties in R.

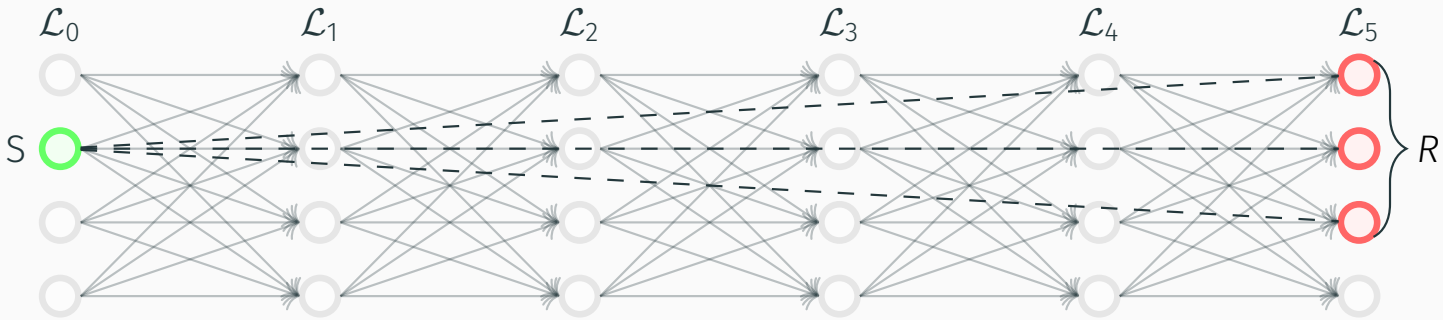
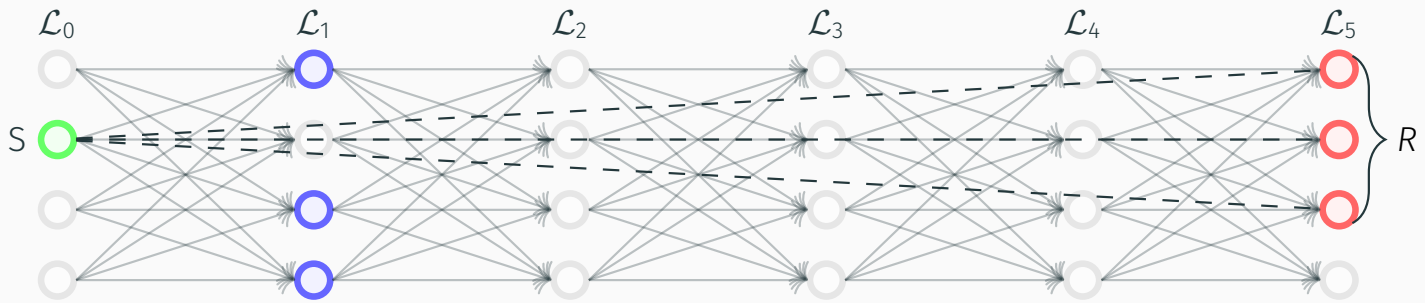


Figure 3: Π_{FMcast} from $S \in \mathcal{L}_0$ of m to $R \subseteq \mathcal{L}_5$

Future Multicast

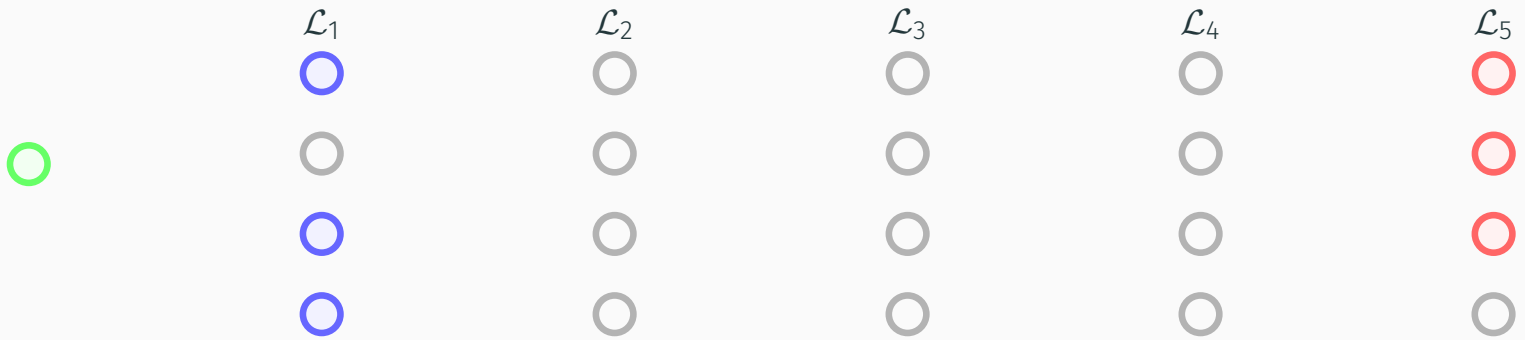
Sketch of Π_{FMcast}

1. S samples additive shares $\{r_T\}_{T \in \mathcal{T}}$ of m.
2. S sends each r_T to $R \subseteq \mathcal{L}_5$ using $\Pi_{\text{weak-FMcast}}$.
   Using a different set of intermediaries $U_T \subset \mathcal{L}_1$ where $|U_T| = n - t$.
3. Parties in $R \subseteq \mathcal{L}_5$ do $\hat{m} = \sum_{T \in \mathcal{T}} \hat{r}_T$.



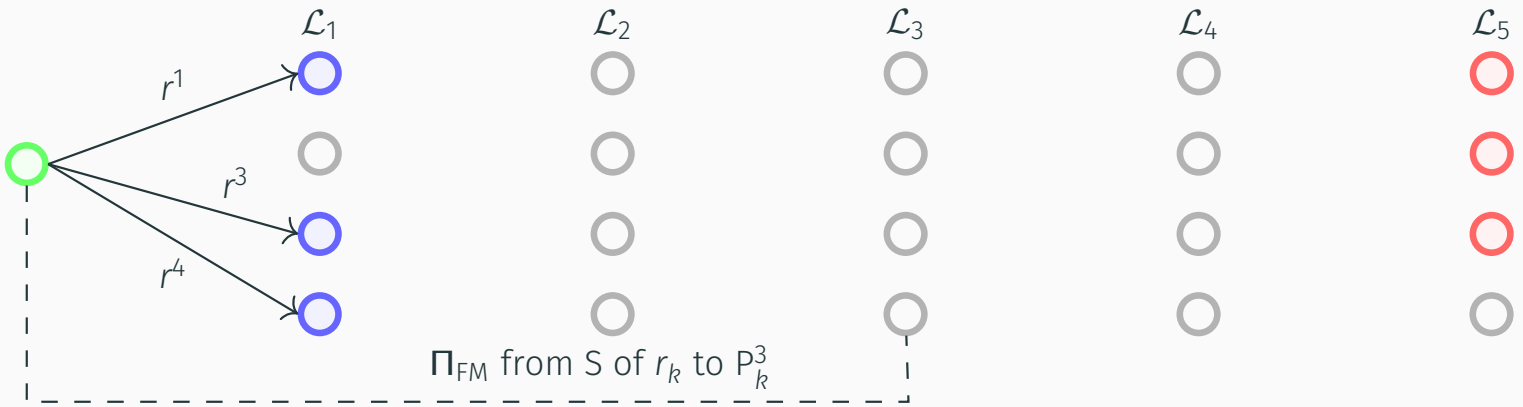
Weak Future Multicast

$\Pi_{\text{weak-FMcast}}$ of $r = r_T$ from $S \in \mathcal{L}_0$ to R using U_T as intermediaries.



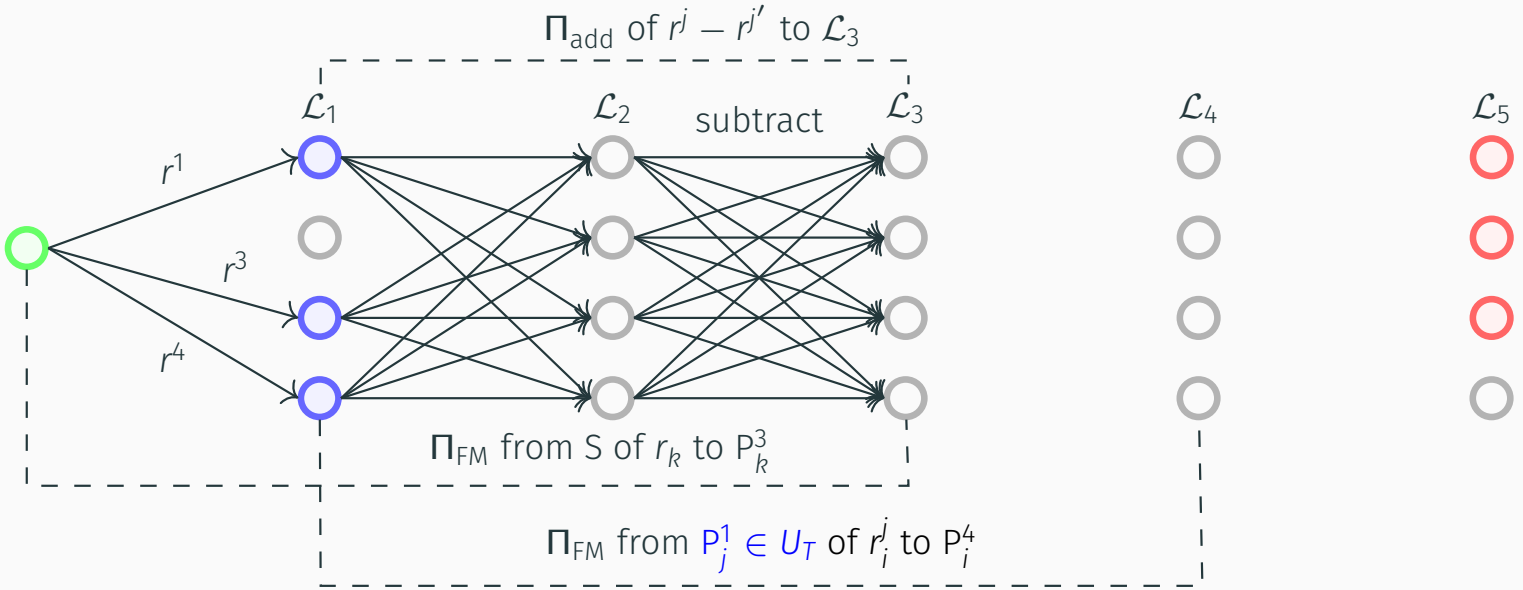
Weak Future Multicast

$\Pi_{\text{weak-FMcast}}$ of $r = r_T$ from $S \in \mathcal{L}_0$ to R using U_T as intermediaries.



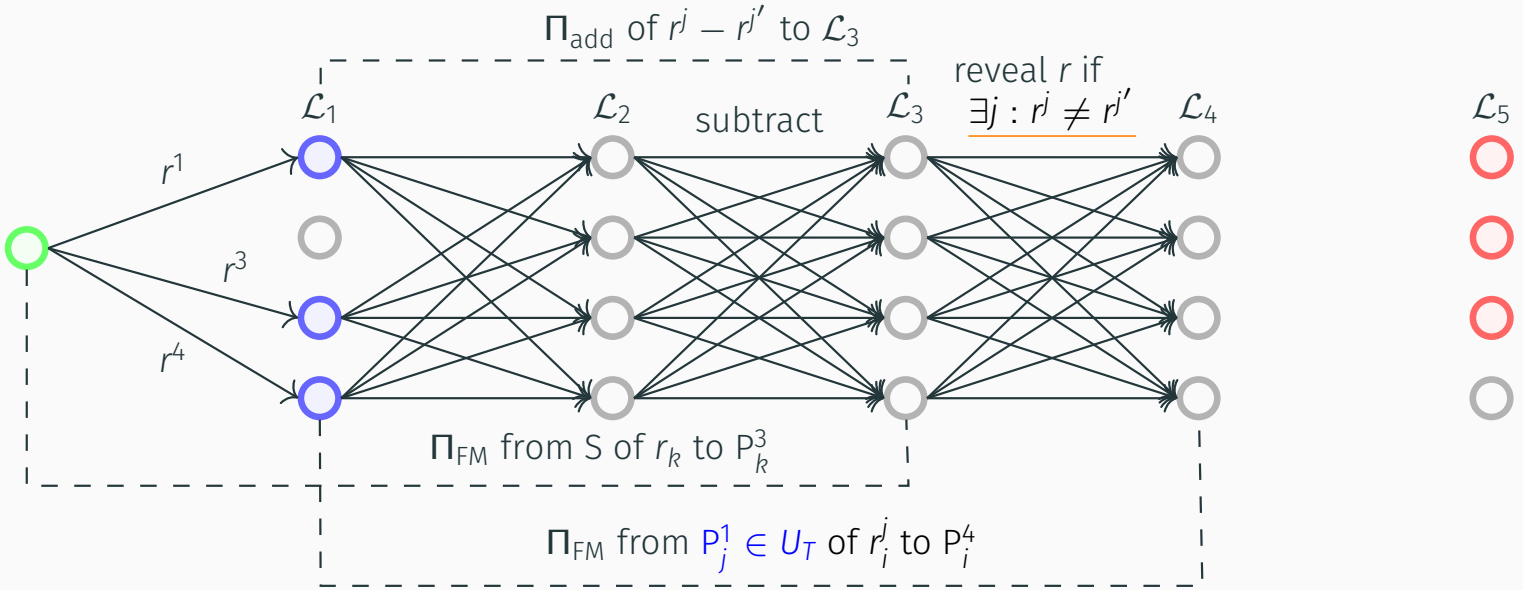
Weak Future Multicast

$\Pi_{\text{weak-FMcast}}$ of $r = r_T$ from $S \in \mathcal{L}_0$ to R using U_T as intermediaries.



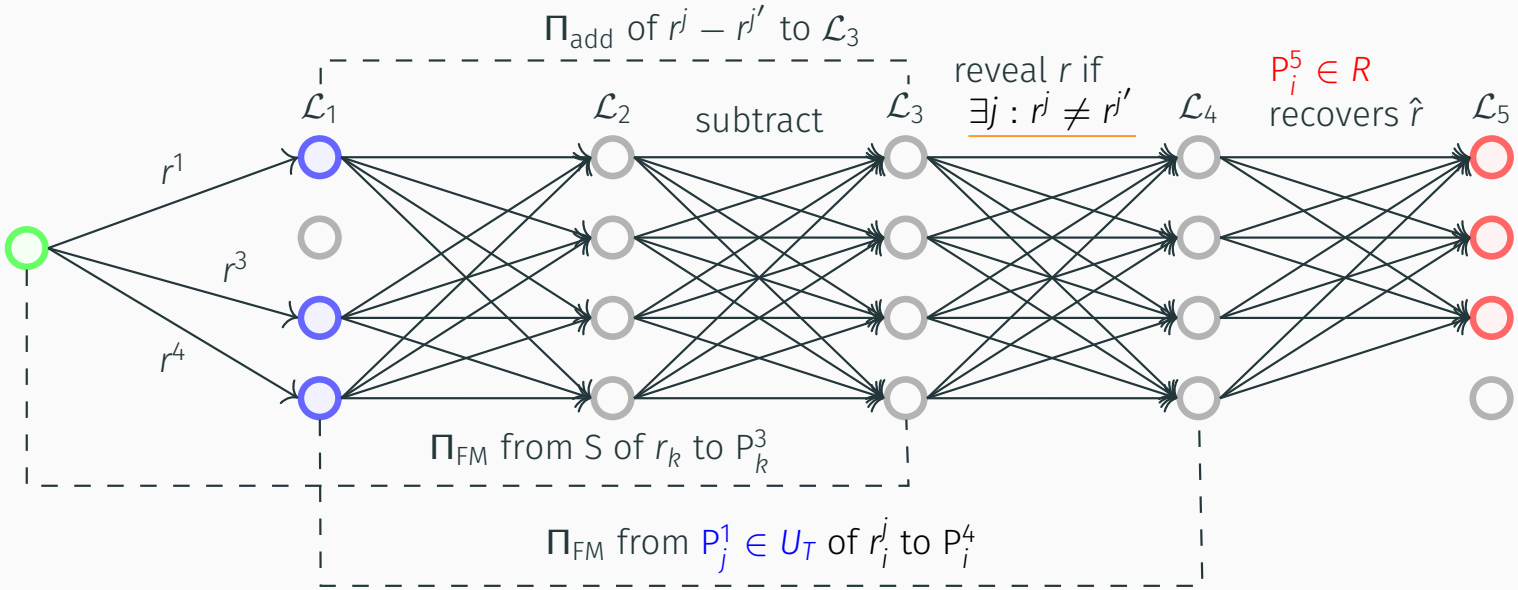
Weak Future Multicast

$\Pi_{\text{weak-FMcast}}$ of $r = r_T$ from $S \in \mathcal{L}_0$ to R using U_T as intermediaries.



Weak Future Multicast

$\Pi_{\text{weak-FMcast}}$ of $r = r_T$ from $S \in \mathcal{L}_0$ to R using U_T as intermediaries.



Layered VSS

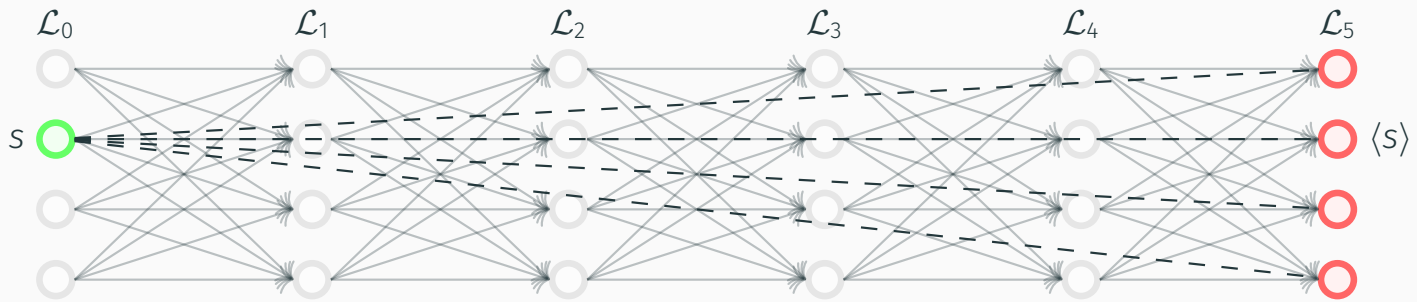
An $(n, t, 5)$-layered protocol Π_{VSS} realizing f_{VSS} where $t < n/3$.

From $\Pi_{\text{weak-FMcast}}$ to Π_{FMcast}:

- Each additive share r_T is transferred to R using U_T.
- Since at least one set (U_T) is comprised of only honest parties the message $m = \sum_{T \in \mathcal{T}} r_T$ remains secure if S and R are honest.

From Π_{FMcast} to Π_{VSS}:

- S samples $\{r_T\}_{T \in \mathcal{T}}$ as additive secret sharing of secret s.
- For each $T \in \mathcal{T}$, execute Π_{FMcast} with S as sender with input r_T and $\{\mathrm{P}_i^5 : i \in T\}$ as receivers.



Results

CNF-based Layered MPC [GIKR01, Mau06]

Theorem 1: CNF-Based Layered MPC

Let f be an n-party functionality computed by a **layered arithmetic circuit** C over a finite ring, with D **layers** and M gates. Then, for any $t < n/3$, there is an $(n, t, O(D))$**-layered MPC protocol** for f. The communication consists of $2^{O(n)} \cdot M$ ring elements.

CNF-based Layered MPC [GIKR01, Mau06]

Theorem 1: CNF-Based Layered MPC

Let f be an n-party functionality computed by a **layered arithmetic circuit** C over a finite ring, with D **layers** and M gates. Then, for any $t < n/3$, there is an $(n, t, O(D))$**-layered MPC protocol** for f. The communication consists of $2^{O(n)} \cdot M$ ring elements.

Corollary 1: Secure Maximally Proactive MPC

Let f be an n-party functionality computed by a layered arithmetic circuit C over a finite ring, **with** D **layers**. Then, for $t < n/3$, there is a **maximally proactive MPC protocol** computing f in $r = O(D)$ **rounds**.

CNF-based Layered MPC [GIKR01, Mau06]

Theorem 1: CNF-Based Layered MPC

Let f be an n-party functionality computed by a **layered arithmetic circuit** C over a finite ring, with D **layers** and M gates. Then, for any $t < n/3$, there is an $(n, t, O(D))$**-layered MPC protocol** for f. The communication consists of $2^{O(n)} \cdot M$ ring elements.

Corollary 1: Secure Maximally Proactive MPC

Let f be an n-party functionality computed by a layered arithmetic circuit C over a finite ring, **with** D **layers**. Then, for $t < n/3$, there is a **maximally proactive MPC protocol** computing f in $r = O(D)$ **rounds**.

- May be concretely efficient for small n.
- Use techniques from [CDI05] to amortize the communication overhead by sending k-bit seeds and let the receivers generate most shares locally.
- This technique makes use of black-box access to PRG (computational security).

Efficient Layered MPC [BGW88]

Theorem 2: Efficient Layered MPC

Let f be an n-party functionality computed by a **layered arithmetic circuit** C over a finite field, with D **layers** and M gates. Then, for any $t < n/3$, there is an $(n, t, O(D))$**-layered MPC protocol** for f. The communication consists of $O(n^9) \cdot M$ field elements.

Efficient Layered MPC [BGW88]

Theorem 2: Efficient Layered MPC

Let f be an n-party functionality computed by a **layered arithmetic circuit** C over a finite field, with D **layers** and M gates. Then, for any $t < n/3$, there is an $(n, t, O(D))$**-layered MPC protocol** for f. The communication consists of $O(n^9) \cdot M$ field elements.

Corollary 2: (Efficient) Secure Maximally Proactive MPC

Let f be an n-party functionality computed by a layered arithmetic circuit C over a finite field, **with** D **layers**. Then, for $t < n/3$, there is an efficient **maximally proactive MPC protocol** computing f in $r = O(D)$ **rounds**.

- Extending the techniques for Distributed Equality Check and Conditional Future Broadcast to the [BGW88]-setting.

Maximally Proactive MPC and Dynamic Committees

f	Reference	Level	Security	Comm.	Threshold
FM	This work	perfect	full	poly(n)	$t < n/3$
VSS	[BGG+20]	comp.	full	poly(n)	$t < n/4^*$
	This work	perfect	full	$2^{O(n)}$	$t < n/3$
	This work (Sec. 5)	perfect	full	poly(n)	$t < n/3$
MPC	[GHK+21] (YOSO)	statistical	full +setup†	poly(n)	$t < n/2^*$
	[CGG+21] (Fluid)	statistical	abort	poly(n)	$t < n/2$
	[OY91]	perfect	full	poly(n)	$t < n/d$
	This work	perfect	full	$2^{O(n)}$	$t < n/3$
	This work (Sec. 5)	perfect	full	poly(n)	$t < n/3$
	This work (Sec. 6)	comp.	full	poly(n)	$t < n/2$

Table 1: Protocols realizing primitives in the most extreme proactive settings. (*protocol security relies on the adversary only doing probabilistic corruption, †assumes access to ideal target-anonymous channels for future messaging)

Conclusion

Summary:

- Definition of MPC over layered graphs (layered MPC).
  - Instance of standard MPC with restricted interaction patterns.
  - Implications for maximally proactive protocols [OY91].
- Reviewed CNF-based layered protocols for f_{VSS}.

Conclusion

Summary:

- Definition of MPC over layered graphs (layered MPC).
  - Instance of standard MPC with restricted interaction patterns.
  - Implications for maximally proactive protocols [OY91].
- Reviewed CNF-based layered protocols for f_{VSS}.
- In Section 5 we describe **efficient** (but more involved) layered protocols for general MPC based on [BGW88].

Conclusion

Summary:

- Definition of MPC over layered graphs (layered MPC).
  - Instance of standard MPC with restricted interaction patterns.
  - Implications for maximally proactive protocols [OY91].
- Reviewed CNF-based layered protocols for f_{VSS}.
- In Section 5 we describe **efficient** (but more involved) layered protocols for general MPC based on [BGW88].
- In Section 6 we present layered protocol for general MPC with **computational** security for $t < n/2$.

Conclusion

Summary:

- Definition of MPC over layered graphs (layered MPC).
  - Instance of standard MPC with restricted interaction patterns.
  - Implications for maximally proactive protocols [OY91].
- Reviewed CNF-based layered protocols for f_{VSS}.
- In Section 5 we describe **efficient** (but more involved) layered protocols for general MPC based on [BGW88].
- In Section 6 we present layered protocol for general MPC with **computational** security for $t < n/2$.

Future Work:

- Identify a **compiler** from a class of protocols secure in the standard setting to secure layered protocols.
- Investigate the **statistical setting** ($t < n/2$) and possibly obtain a full characterization of layered MPC.

Thank You!

Check out the eprint:
https://ia.cr/2023/330 & https://ia.cr/2023/415

References i


J. Baron, K. El Defrawy, J. Lampkins, and R. Ostrovsky.
How to withstand mobile virus attacks, revisited.
In *33rd ACM PODC*, pages 293–302. ACM, July 2014.


F. Benhamouda, C. Gentry, S. Gorbunov, S. Halevi, H. Krawczyk, C. Lin, T. Rabin, and L. Reyzin.
Can a public blockchain keep a secret?
In *TCC 2020, Part I*, *LNCS* 12550, pages 260–290. Springer, Heidelberg, November 2020.


M. BenOr, S. Goldwasser, and A. Wigderson.
Completeness theorems for non-cryptographic fault-tolerant distributed computation.
In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 351–371. 1988.

References ii

R. Canetti.
Security and composition of multiparty cryptographic protocols.

Journal of CRYPTOLOGY, 13(1):143–202, 2000.

R. Cramer, I. Damgård, and Y. Ishai.
Share conversion, pseudorandom secret-sharing and applications to secure computation.
In *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, *Lecture Notes in Computer Science* 3378, pages 342–362. Springer, 2005.

References iii

A. R. Choudhuri, A. Goel, M. Green, A. Jain, and G. Kaptchuk.
Fluid MPC: Secure multiparty computation with dynamic participants.
In *CRYPTO 2021, Part II*, *LNCS* 12826, pages 94–123, Virtual Event, August 2021. Springer, Heidelberg.

R. Canetti and A. Herzberg.
Maintaining security in the presence of transient faults.
In *Advances in Cryptology—CRYPTO'94: 14th Annual International Cryptology Conference Santa Barbara, California, USA August 21–25, 1994 Proceedings*, pages 425–438. Springer, 2001.

References iv


C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strobl.
Asynchronous verifiable secret sharing and proactive cryptosystems.
In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 88–97, 2002.


D. Dolev, C. Dwork, O. Waarts, and M. Yung.
Perfectly secure message transmission.
Journal of the ACM (JACM), 40(1):17–47, 1993.


Y. Desmedt and S. Jajodia.
Redistributing secret shares to new access structures and its applications.
Technical report, Citeseer, 1997.

References v

K. Eldefrawy, T. Lepoint, and A. Leroux.
Communication-efficient proactive secret sharing for dynamic groups with dishonest majorities.
In *ACNS 20, Part I*, *LNCS* 12146, pages 3–23. Springer, Heidelberg, October 2020.

J. A. Garay.
Reaching (and maintaining) agreement in the presence of mobile faults.
In *International Workshop on Distributed Algorithms*, pages 253–264. Springer, 1994.

References vi

C. Gentry, S. Halevi, H. Krawczyk, B. Magri, J. B. Nielsen, T. Rabin, and S. Yakoubov.
YOSO: You only speak once - secure MPC with stateless ephemeral roles.
In *CRYPTO 2021, Part II*, *LNCS* 12826, pages 64–93, Virtual Event, August 2021. Springer, Heidelberg.

Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich.
Algorand: Scaling byzantine agreements for cryptocurrencies.
In *Proceedings of the 26th Symposium on Operating Systems Principles*, pages 51–68, 2017.

References vii


R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin.
The round complexity of verifiable secret sharing and secure multicast.
In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 580–589, 2001.


O. Goldreich.
Foundations of cryptography: volume 2, basic applications.
Cambridge university press, 2009.


S. Halevi, Y. Ishai, A. Jain, E. Kushilevitz, and T. Rabin.
Secure multiparty computation with general interaction patterns.
In *ITCS 2016*, pages 157–168. ACM, January 2016.

References viii

A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung.
Proactive secret sharing or: How to cope with perpetual leakage.
In *CRYPTO'95*, *LNCS* 963, pages 339–352. Springer, Heidelberg, August 1995.

M. Hirt and U. M. Maurer.
Player simulation and general adversary structures in perfect multiparty computation.
J. Cryptol., 13(1):31–60, 2000.

U. Maurer.
Secure multi-party computation made simple.
Discrete Applied Mathematics, 154(2):370–381, 2006.

References ix


S. K. D. Maram, F. Zhang, L. Wang, A. Low, Y. Zhang, A. Juels, and D. Song.
CHURP: Dynamic-committee proactive secret sharing.
In *ACM CCS 2019*, pages 2369–2386. ACM Press, November 2019.


R. Ostrovsky and M. Yung.
How to withstand mobile virus attacks (extended abstract).
In *10th ACM PODC*, pages 51–59. ACM, August 1991.


T. Rabin and M. BenOr.
Verifiable secret sharing and multiparty protocols with honest majority.
In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 73–85, 1989.

References x


T. M. Wong, C. Wang, and J. M. Wing.
Verifiable secret redistribution for archive systems.
In *First International IEEE Security in Storage Workshop, 2002. Proceedings.*, pages 94–105. IEEE, 2002.