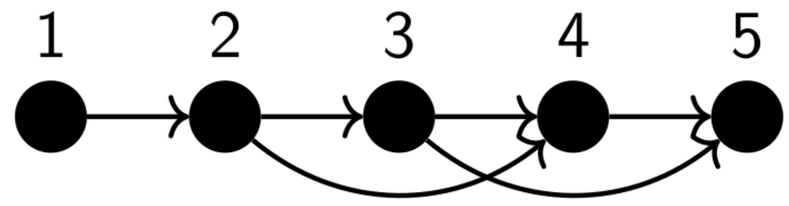
A New Connection Between Node and Edge Depth Robust Graphs

Jeremiah Blocki, Mike Cinkoske

Purdue University

What are Depth Robust graphs?

- **Def:** An (e, d)-node-depth-robust (resp. edge-depth-robust) graph is a directed acyclic graph (DAG) with the property that if any e nodes (resp. edges) are removed, there there exists a path of length at least d in the removed graph.
- Highly depth robust graphs necessary [AB16] and sufficient [ABP17] for creating secure Memory Hard Functions.
- Also used for Proofs of Space and Proofs of Sequential Work.



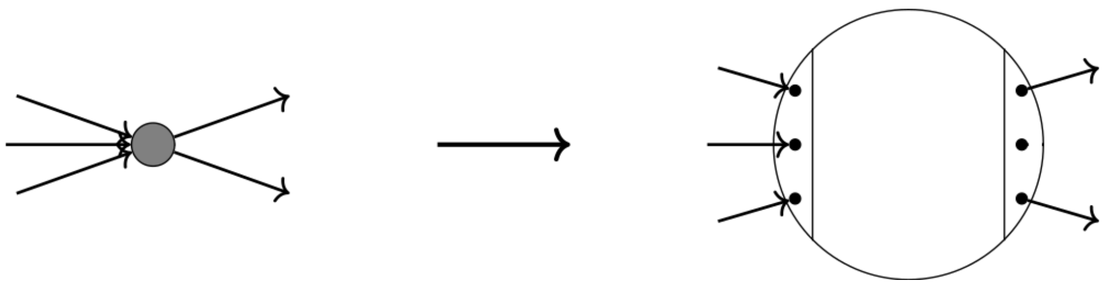
Graph is (1,3)-node-depth-robust and (1, 4)-edge-depth-robust.

Our Transformation

- Generally want node depth robust graphs with constant indegree in applications.
- Removing an edge causes less change than removing a node.
- Edge depth robust graphs could be easier to construct
- Want to transform an edge depth robust graph into a node depth robust graph.

Our Idea

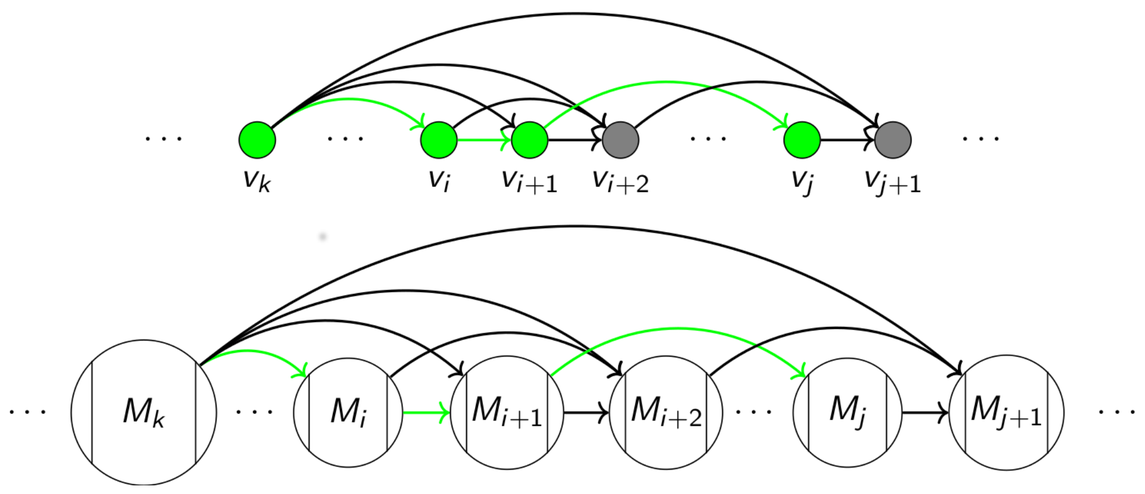
1. Take a highly edge depth robust graph G.
2. Replace each node of G with an ST-robust graph that has constant indegree.
3. Resulting graph has constant indegree and is highly node depth robust.



The size of the replacement graph is proportional to the max of the indegree and outdegree of the node.

Main Theorem

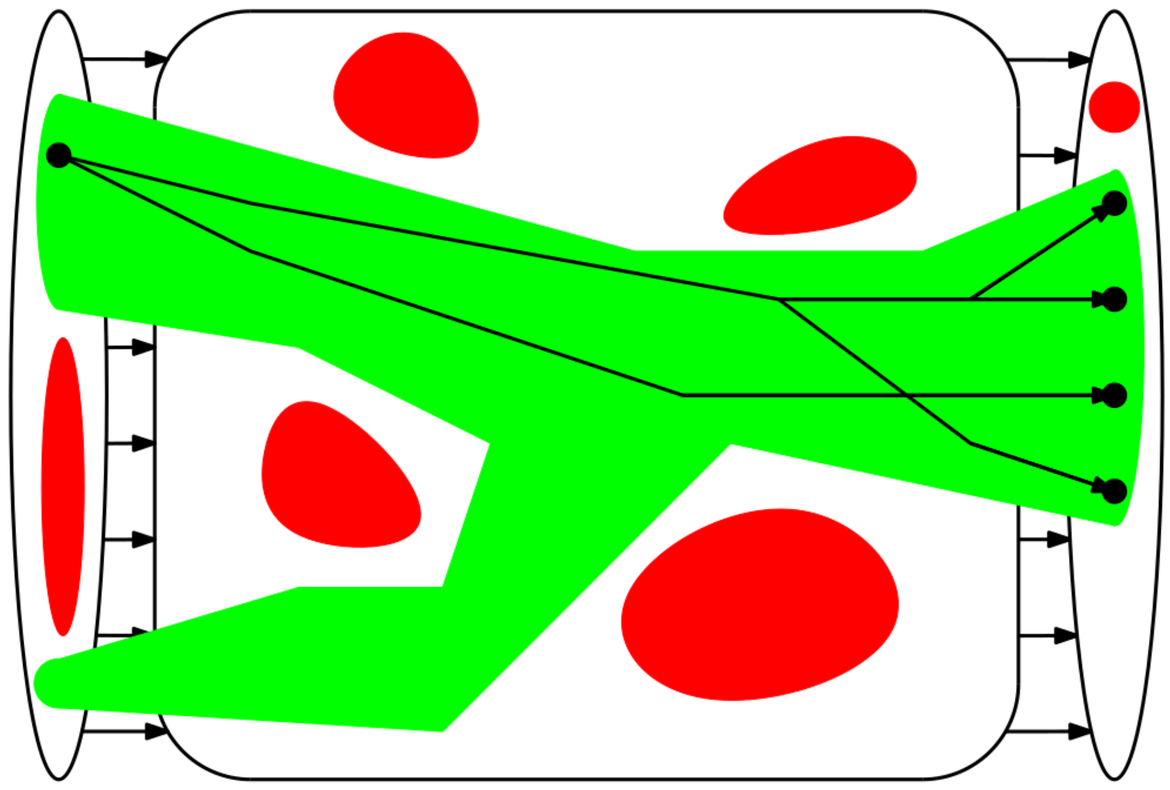
- If G is an (e, d)-edge-depth-robust graph with m edges, then there exists G' which is $(e/4, d)$-depth-robust with $O(m)$ nodes and constant indegree.
- Each path in original graph corresponds to a path in the transformed graph.
- Removing a node from an ST-robust graph is equivalent to removing two edges from original graph.



Paths in original graph correspond to paths in the transformed graph.

ST-Robust Graphs

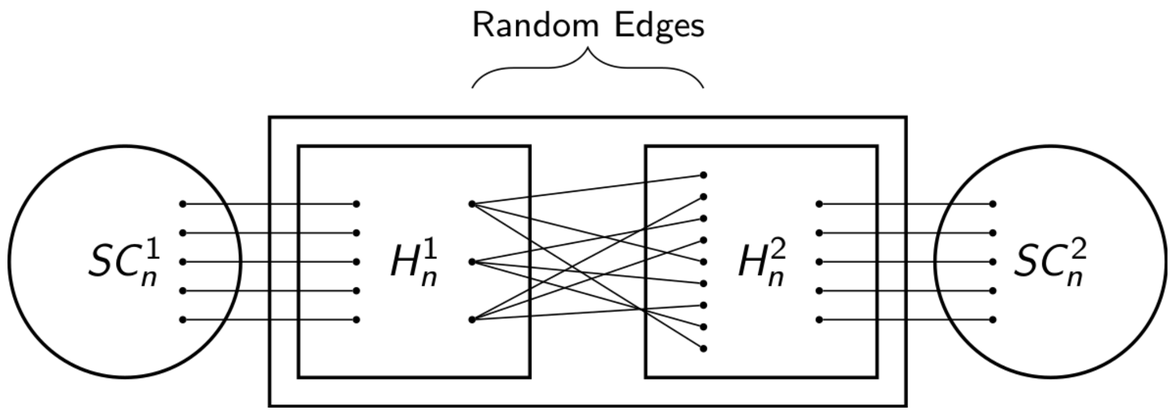
- **Def:** A DAG G is (k_1, k_2)-ST-robust if we remove k_1 nodes and there exists a subgraph with at least k_2 inputs and k_2 outputs, such that each input is connected to every output.
- **Def:** Say G is max ST-robust if G is $(k, n-k)$-ST-robust for all $0 \leq k \leq n$.
- Easy to make with max ST-robust graphs with $O(n \log n)$ nodes and constant indegree.



Remove k_1 nodes and each of the k_2 inputs is connected to all k_2 outputs.

Constructing ST-Robust Graphs

- Want max ST-robust graphs with $O(n)$ nodes and constant indegree.
- H_n^i are highly node depth robust with constant indegree.
- SC_n^i are linear-sized, constant indegree superconcentrators.
- Connect sides by $O(n)$ randomly selected edges.



Construction of a max ST-robust graph with $O(n)$ nodes and constant indegree

Results

- Need node depth robust graph with certain parameters to construct optimal iMHF. Remove $n \log\log n / \log n$ nodes, want maximum d.
- Apply our transformation to graph from [Sch83] and get $(\frac{N \log\log N}{\log N}, \frac{N}{\log N (\log N)^{\log\log N}})$-node-depth-robust graph.
- Previous best was $(\frac{N \log\log N}{\log N}, n^{1-\epsilon})$-node-depth-robust.

References

[AB16] Joël Alwen and Jeremiah Blocki.
Efficiently computing data-independent memory-hard functions.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 241–271. Springer, Heidelberg, August 2016.

[ABP17] Joël Alwen, Jeremiah Blocki, and Krzysztof Pietrzak.
Depth-robust graphs and their cumulative memory complexity.
In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part III*, volume 10212 of *LNCS*, pages 3–32. Springer, Heidelberg, April / May 2017.

[Sch83] Georg Schnitger.
On depth-reduction and grates.
In *24th Annual Symposium on Foundations of Computer Science, Tucson, Arizona, USA, 7-9 November 1983*, pages 323–328. IEEE Computer Society, 1983.

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 | Alexandria, Virginia