Valiant's Universal Circuit is Practical

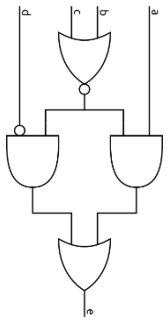
Ágnes Kiss
Thomas Schneider

TU Darmstadt

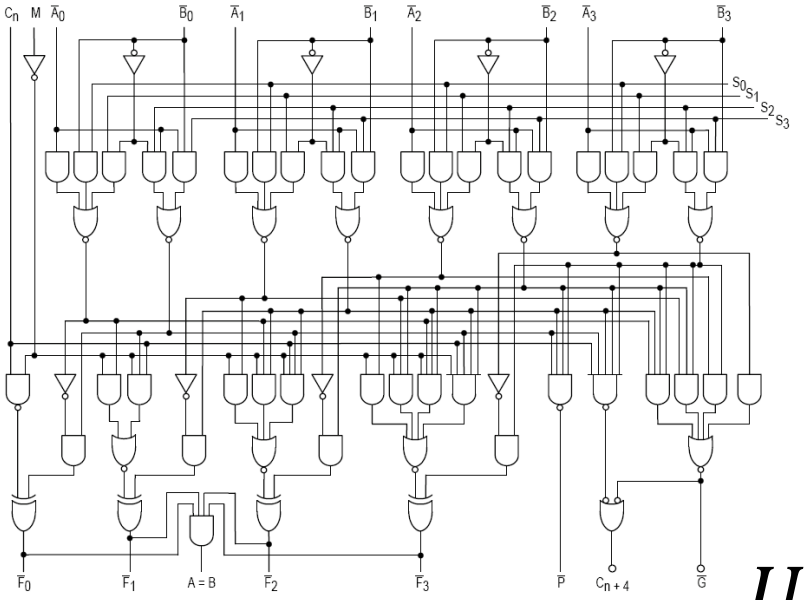
Eurocrypt 2016
May 11, 2016

Universal Circuit (UC)

There is a Boolean circuit UC of size $O(n \log n)$
for which it holds that
for any Boolean function f of size n
UC can be made to compute f.



f



UC

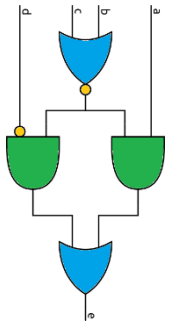
Leslie G. Valiant
1976

Universal Circuit (UC)

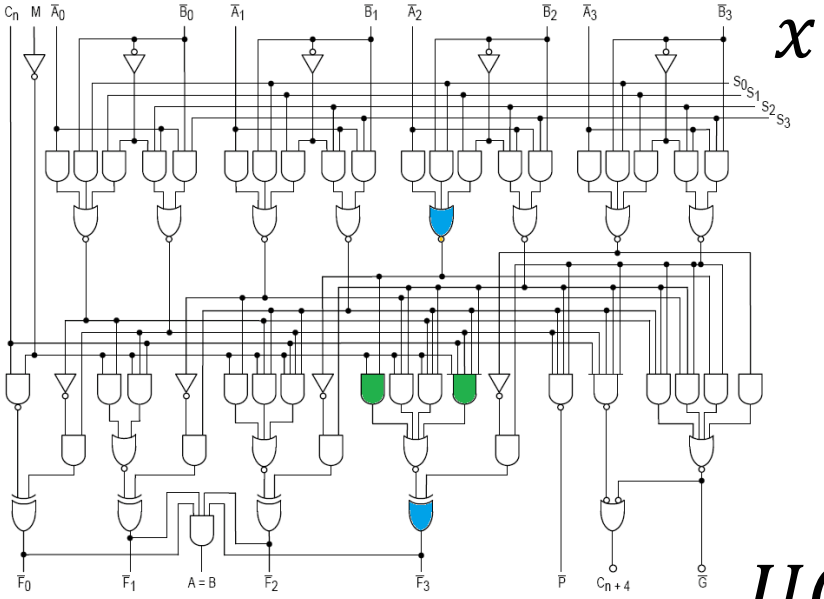
There is a Boolean circuit UC of size $O(n \log n)$
for which it holds that
for any Boolean function f of size n
there exists a programming p
such that for any input x: $UC(p, x) = f(x)$.

Leslie G. Valiant
1976

x p x



$f(x)$



$UC(p, x)$

UC Applications

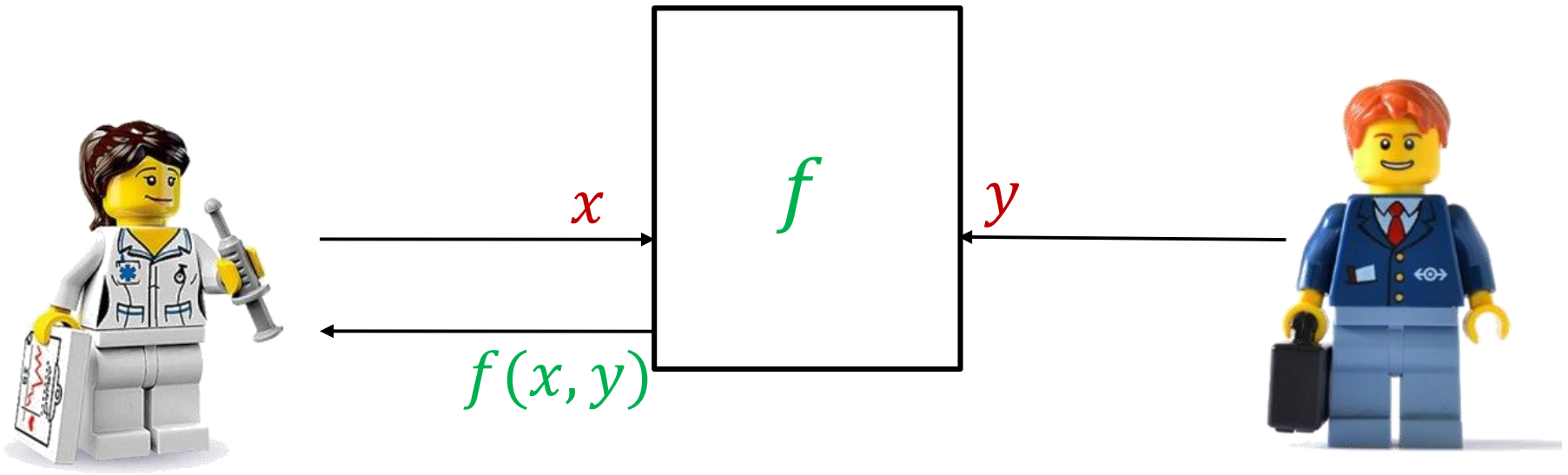
Verifiable computation

Program obfuscation

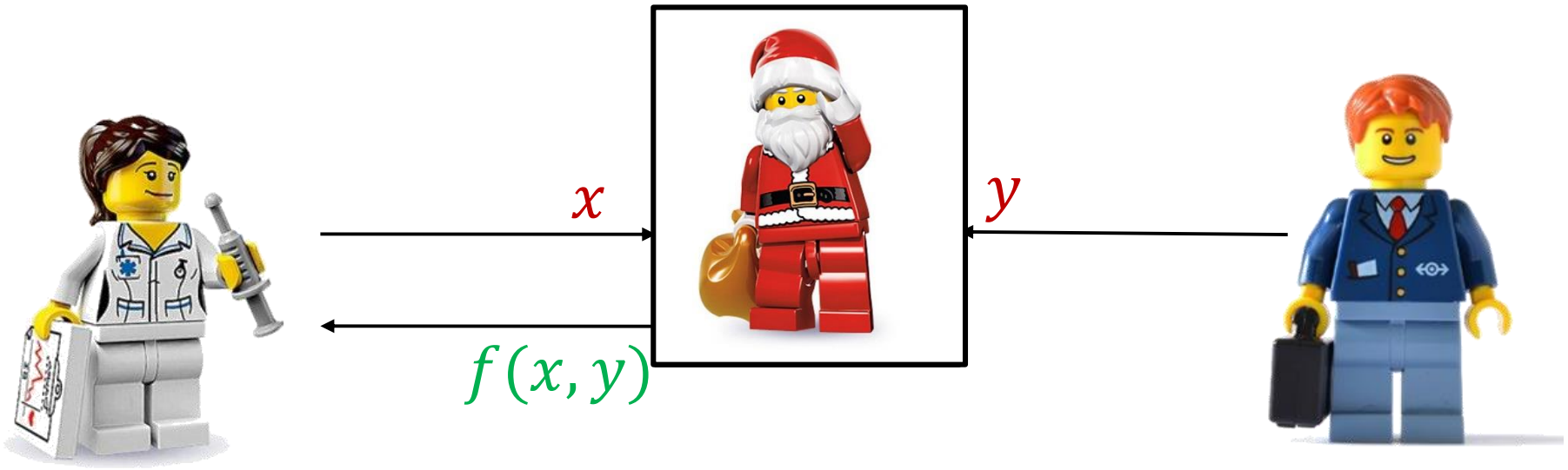
Attribute-based encryption

Private function evaluation

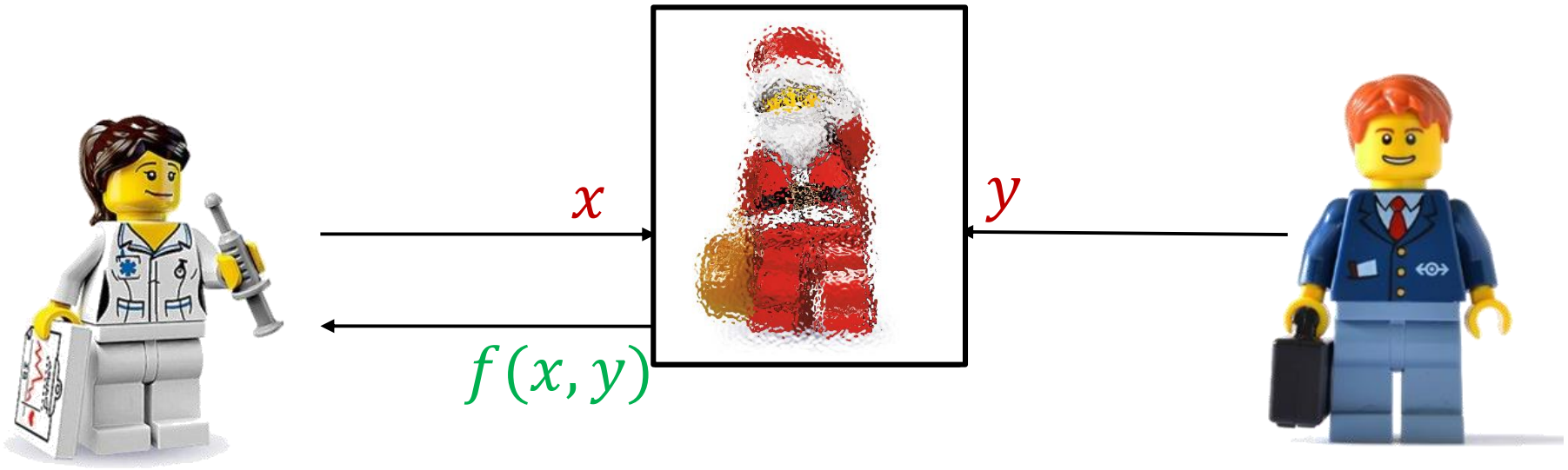
Secure Function Evaluation



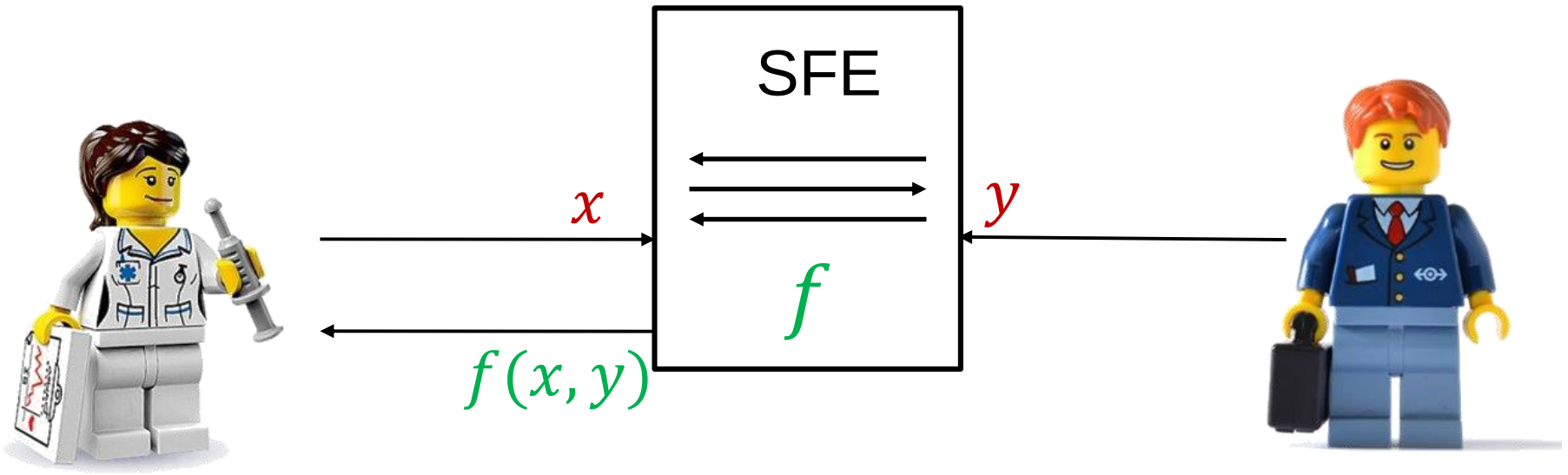
Secure Function Evaluation



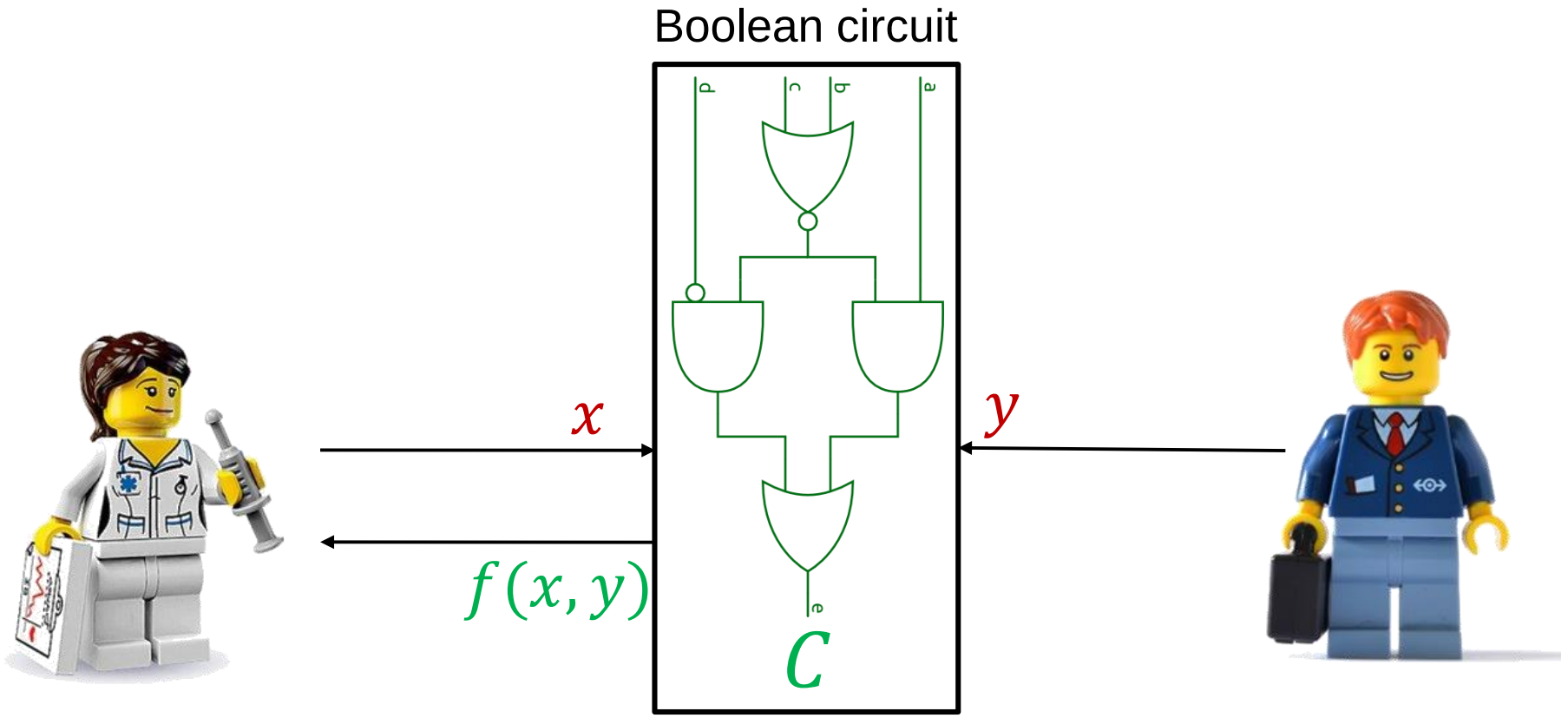
Secure Function Evaluation



Secure Function Evaluation

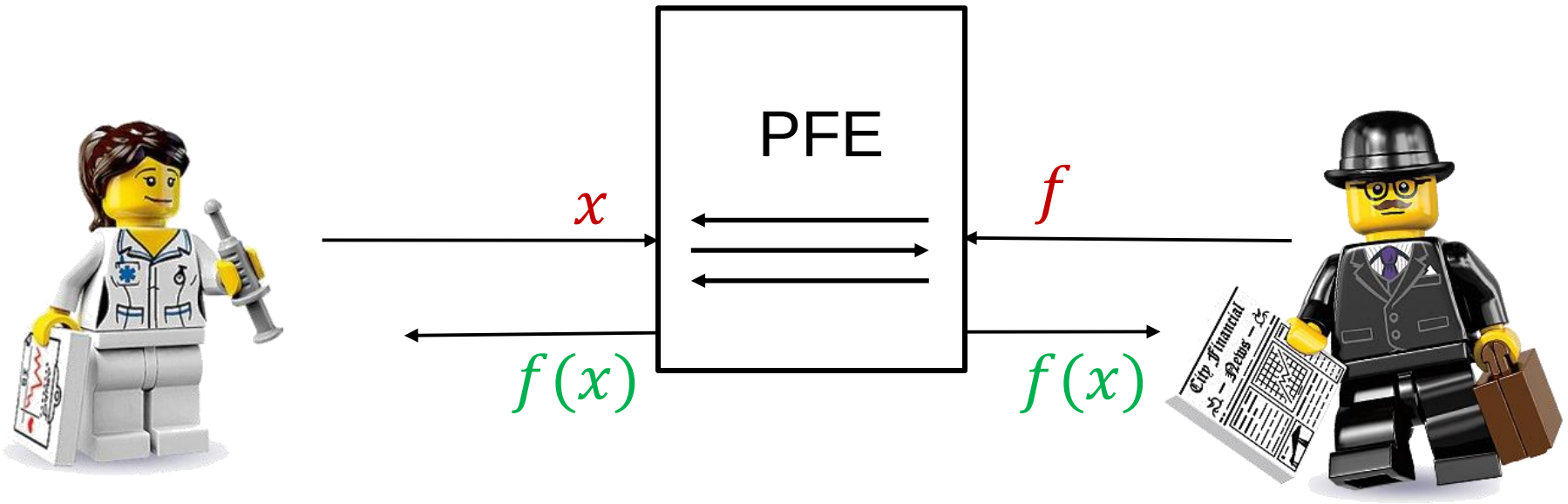


Secure Function Evaluation

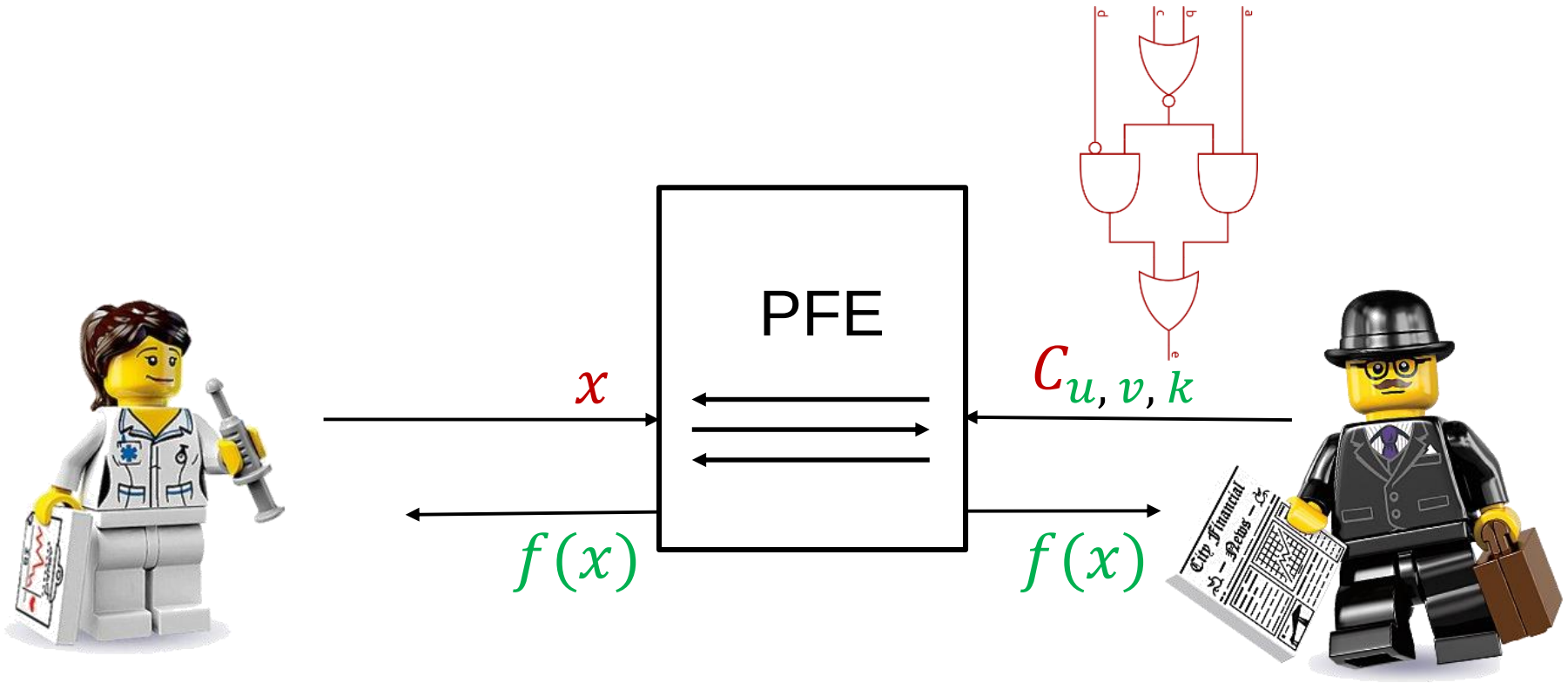


- ⇨ Yao's Garbled Circuit Protocol
- ⇨ Goldreich-Micali-Wigderson Protocol

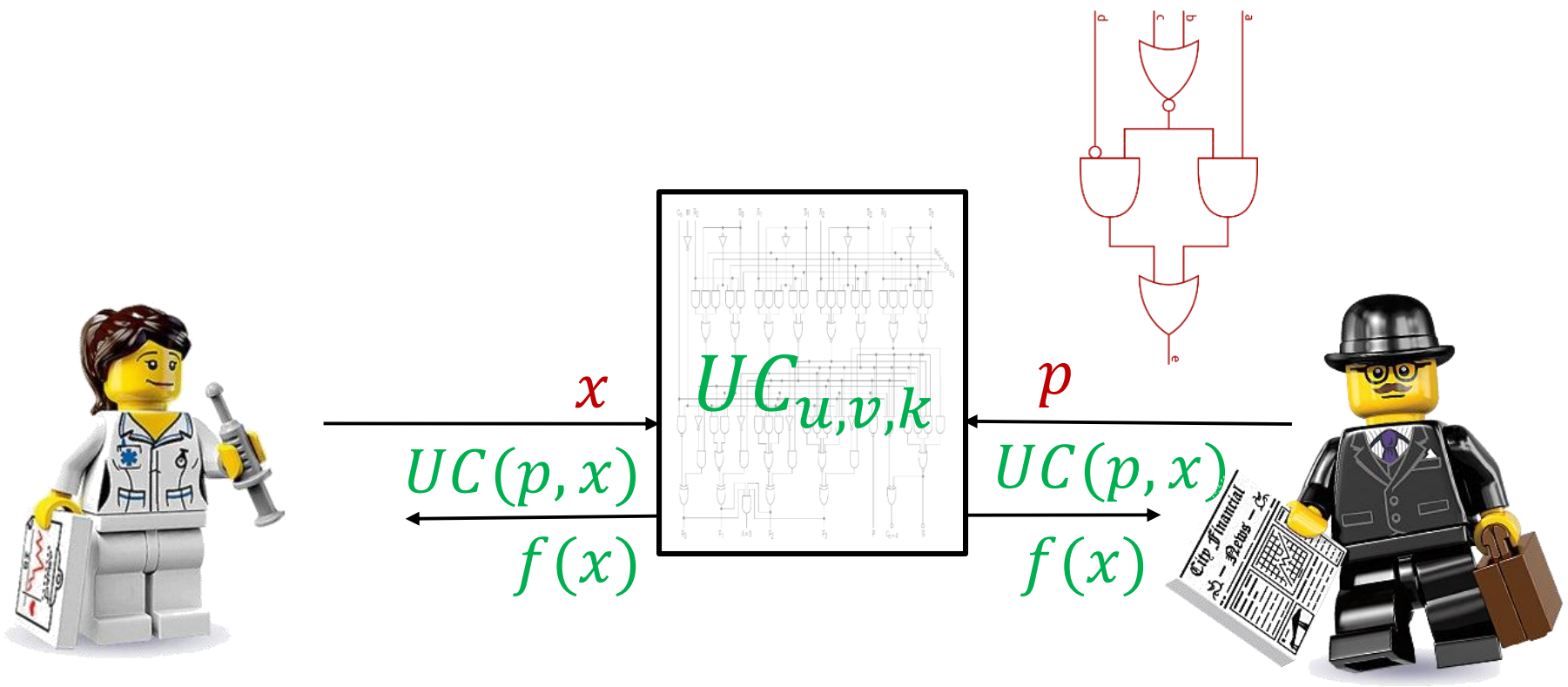
Private Function Evaluation



Private Function Evaluation



Private Function Evaluation



PFE Applications

Software diagnostics

Medical diagnostics

Private databases

Private search queries

UC Construction

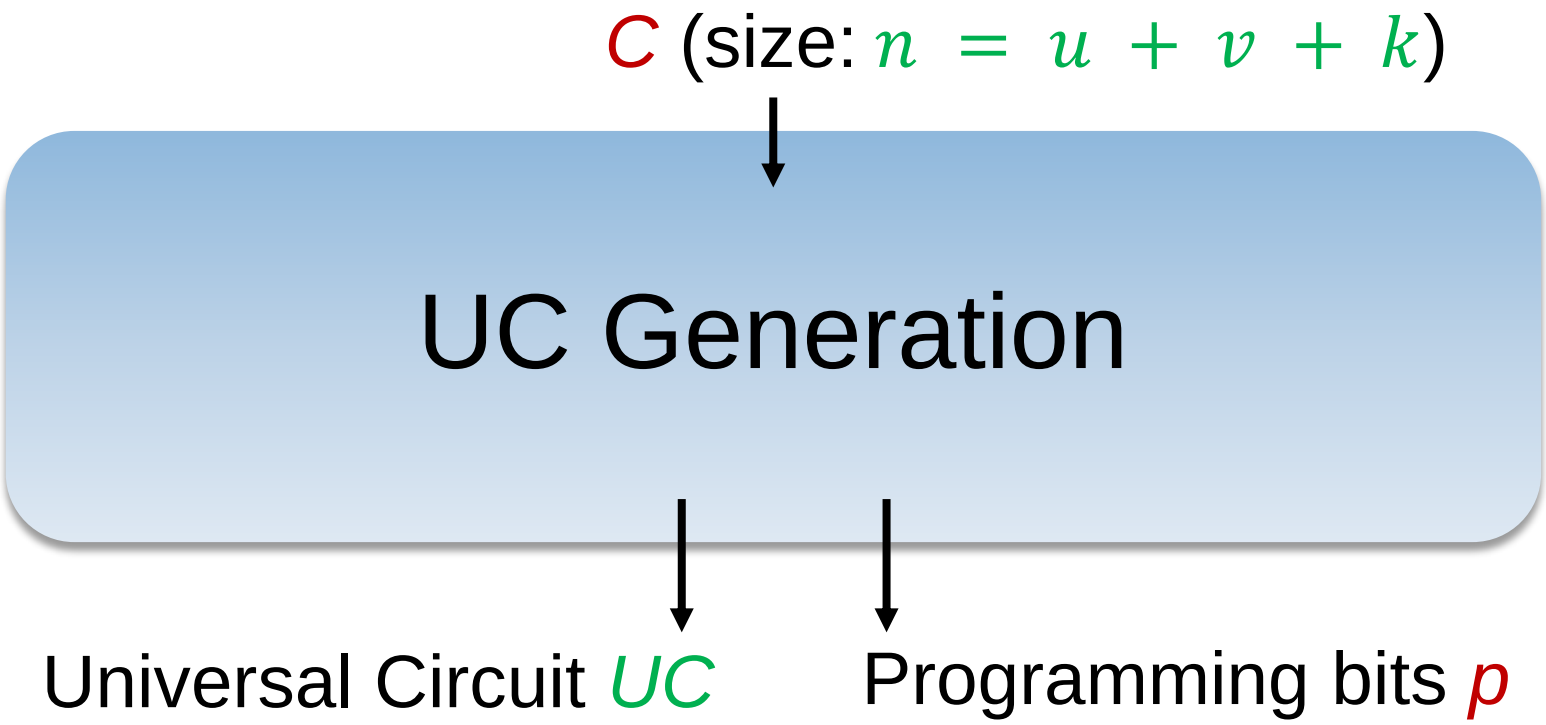
C (size: $n = u + v + k$)

UC Construction

C (size: $n = u + v + k$)

UC Generation

UC Construction



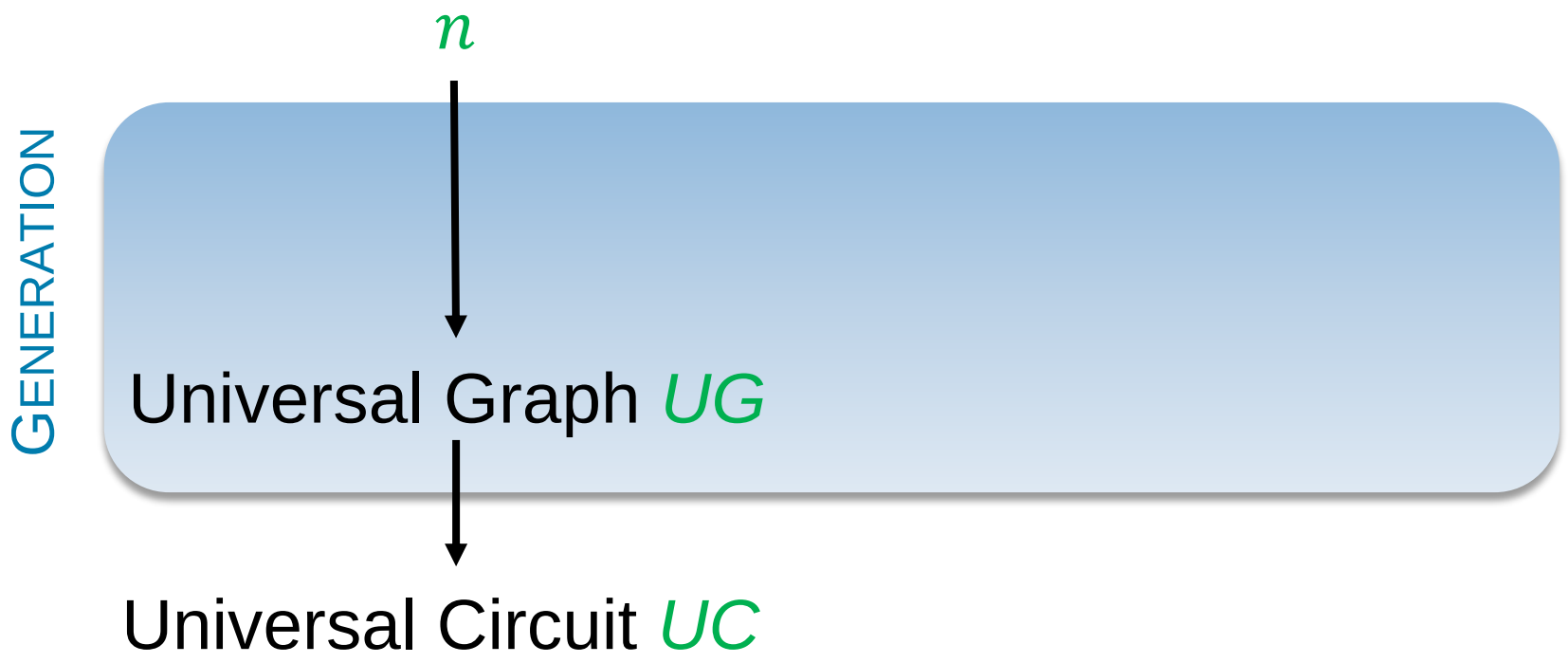
Existing UC Constructions

	[Val76]	[KS08]
Size	$O(n \log n)$	$O(n \log^2 n)$
Depth	$O(n)$	$O(n \log n)$
Implemented	✗	✓

[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

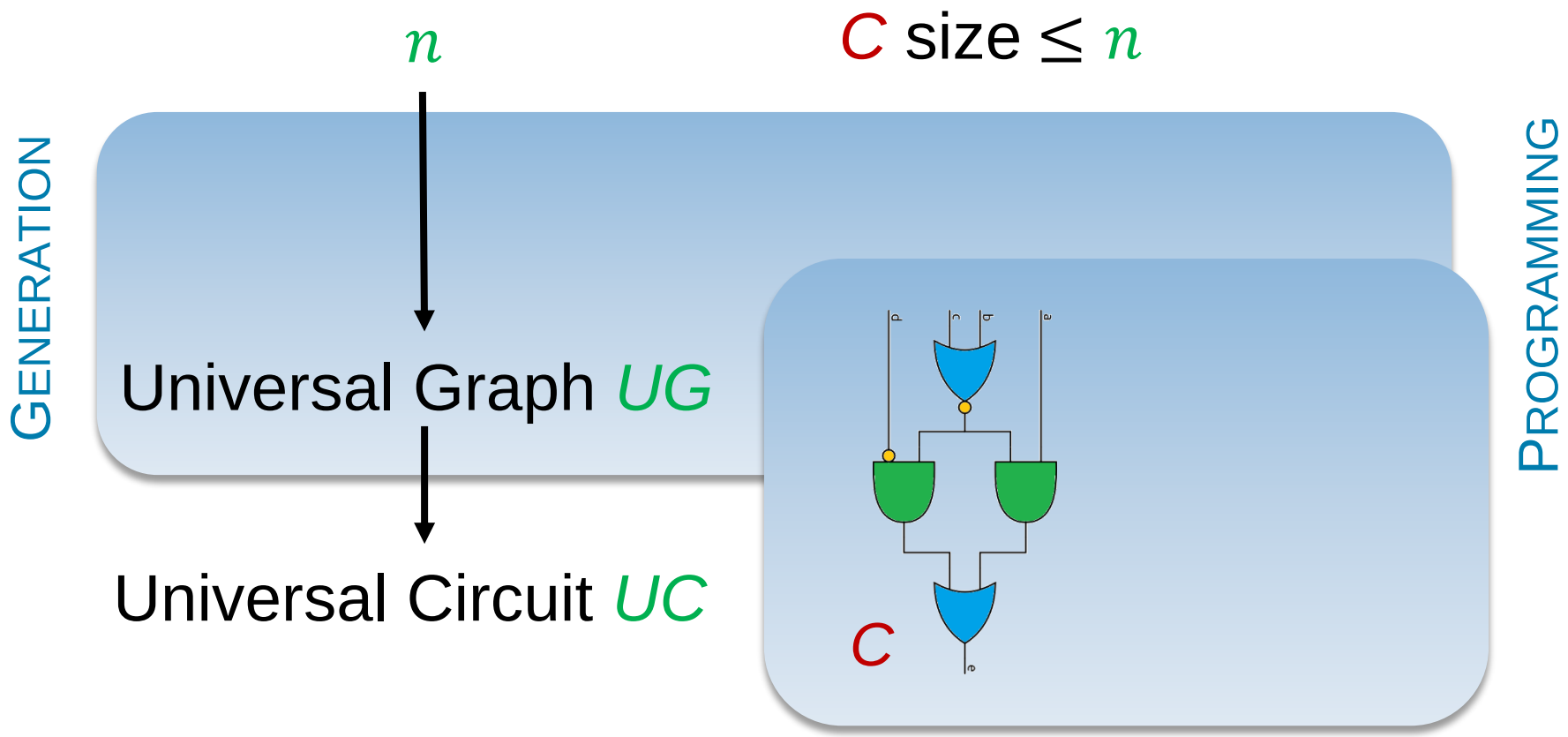
[KS08] V. Kolesnikov, T. Schneider: A practical universal circuit construction and secure evaluation of private functions. In *FC 2008*.

Valiant's UC Construction



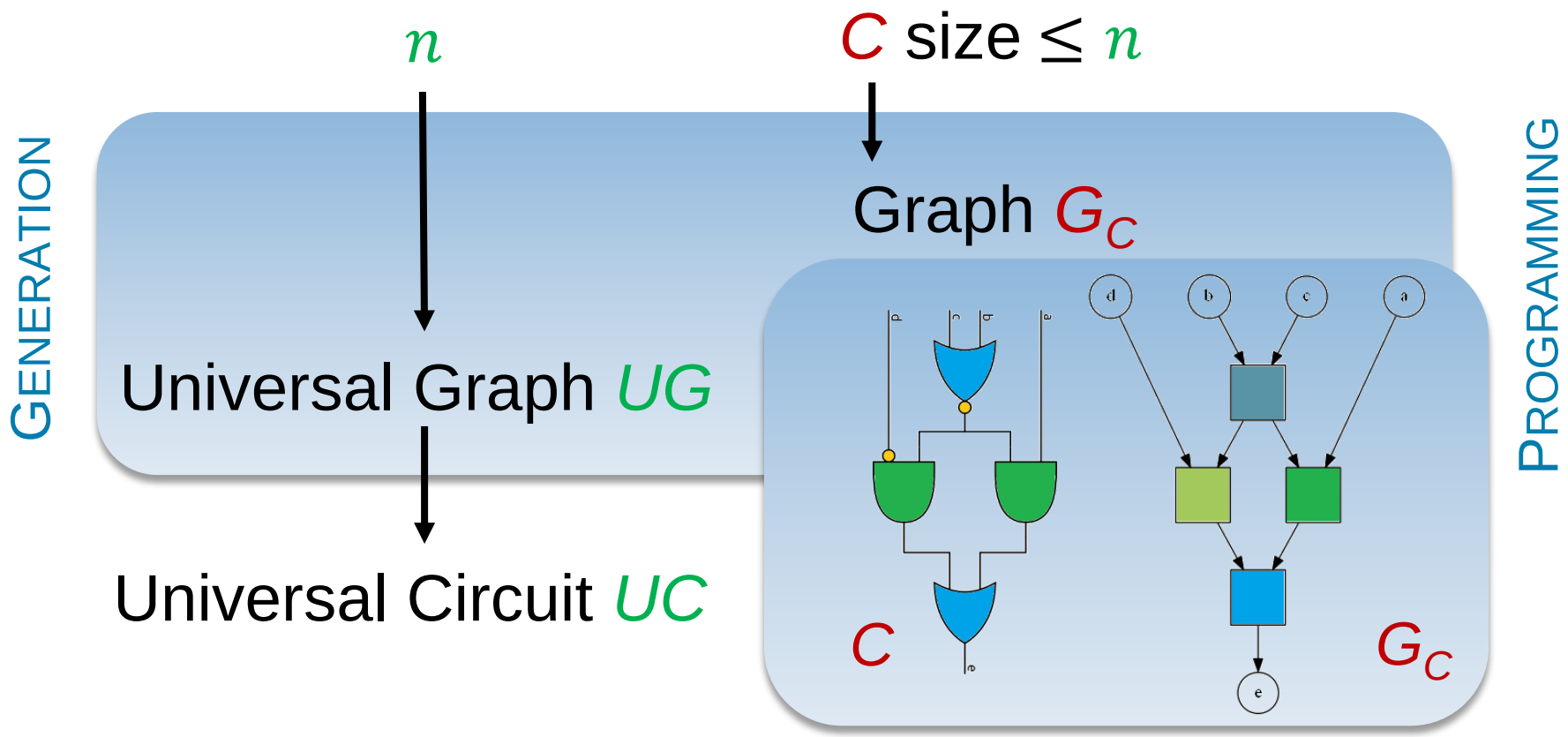
[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Valiant's UC Construction



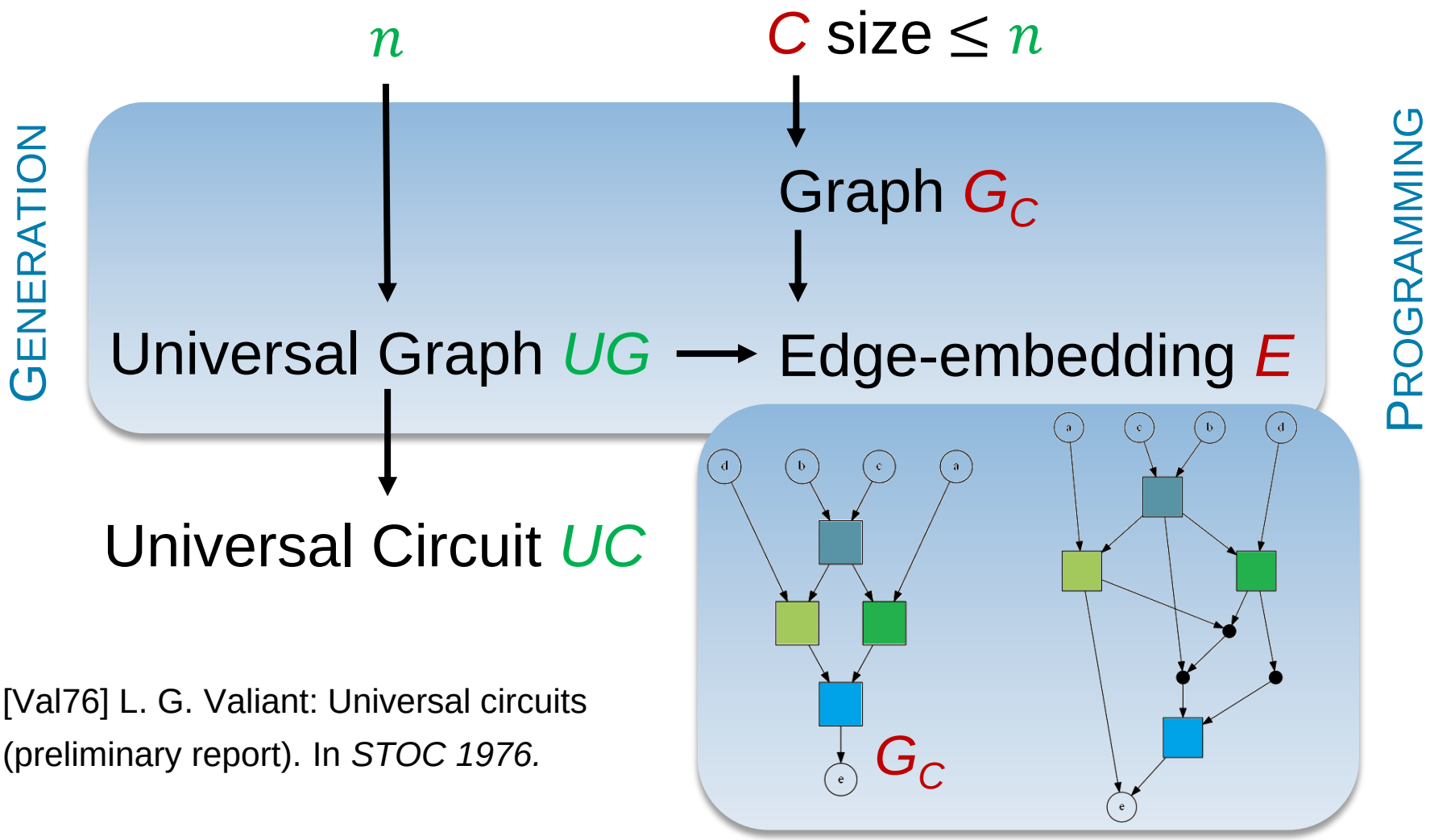
[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Valiant's UC Construction



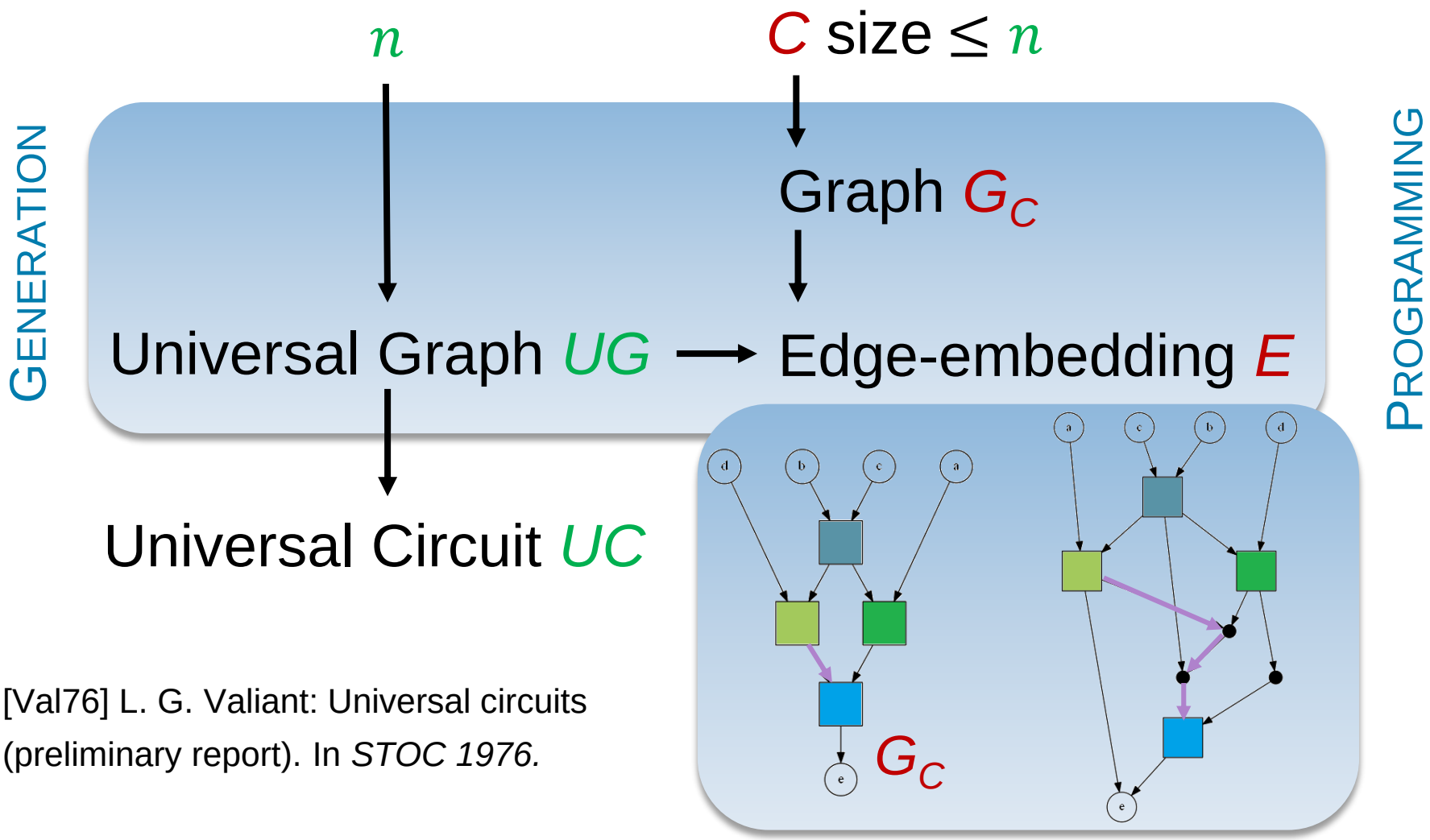
[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Valiant's UC Construction



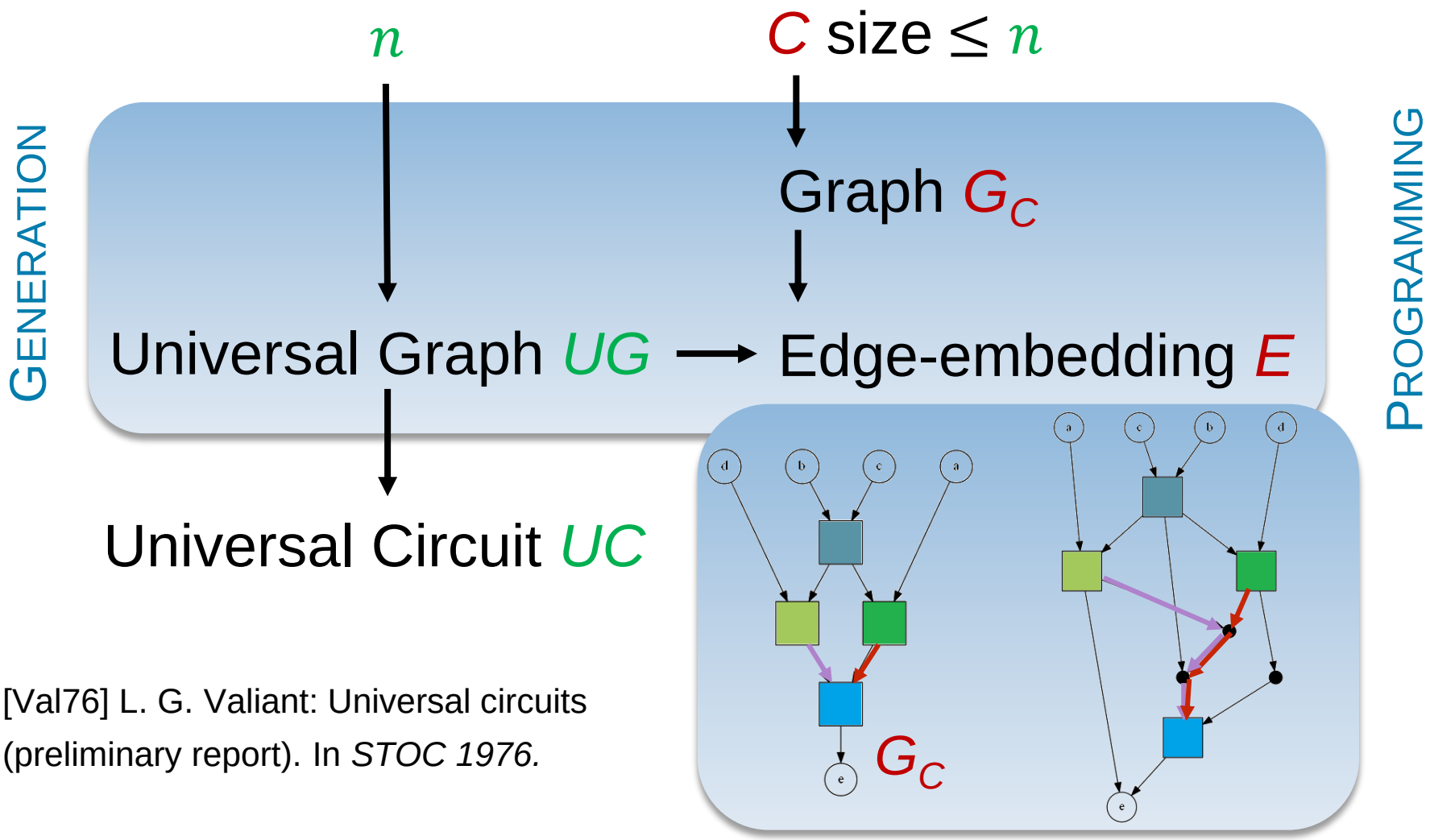
[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Valiant's UC Construction



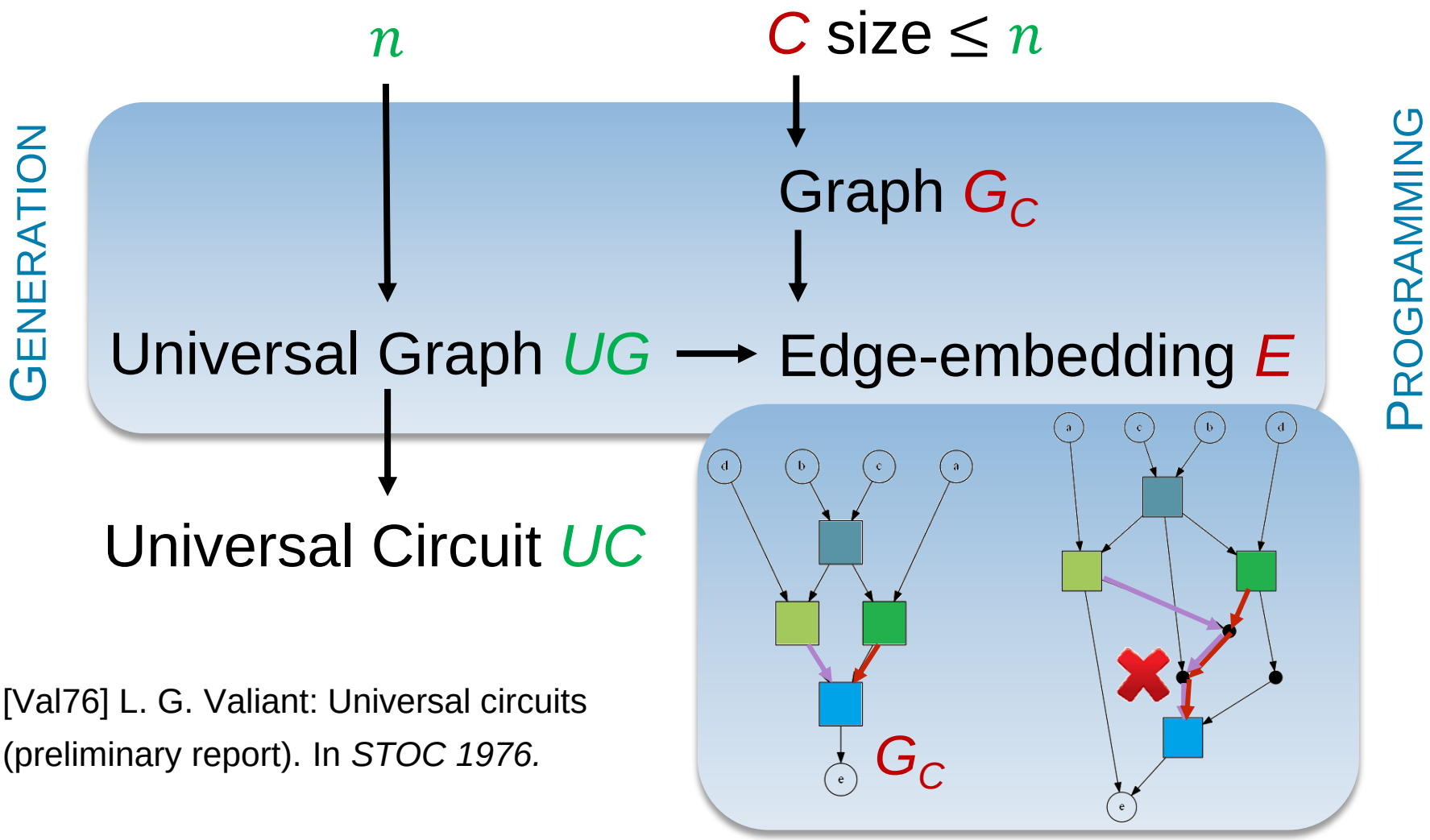
[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Valiant's UC Construction



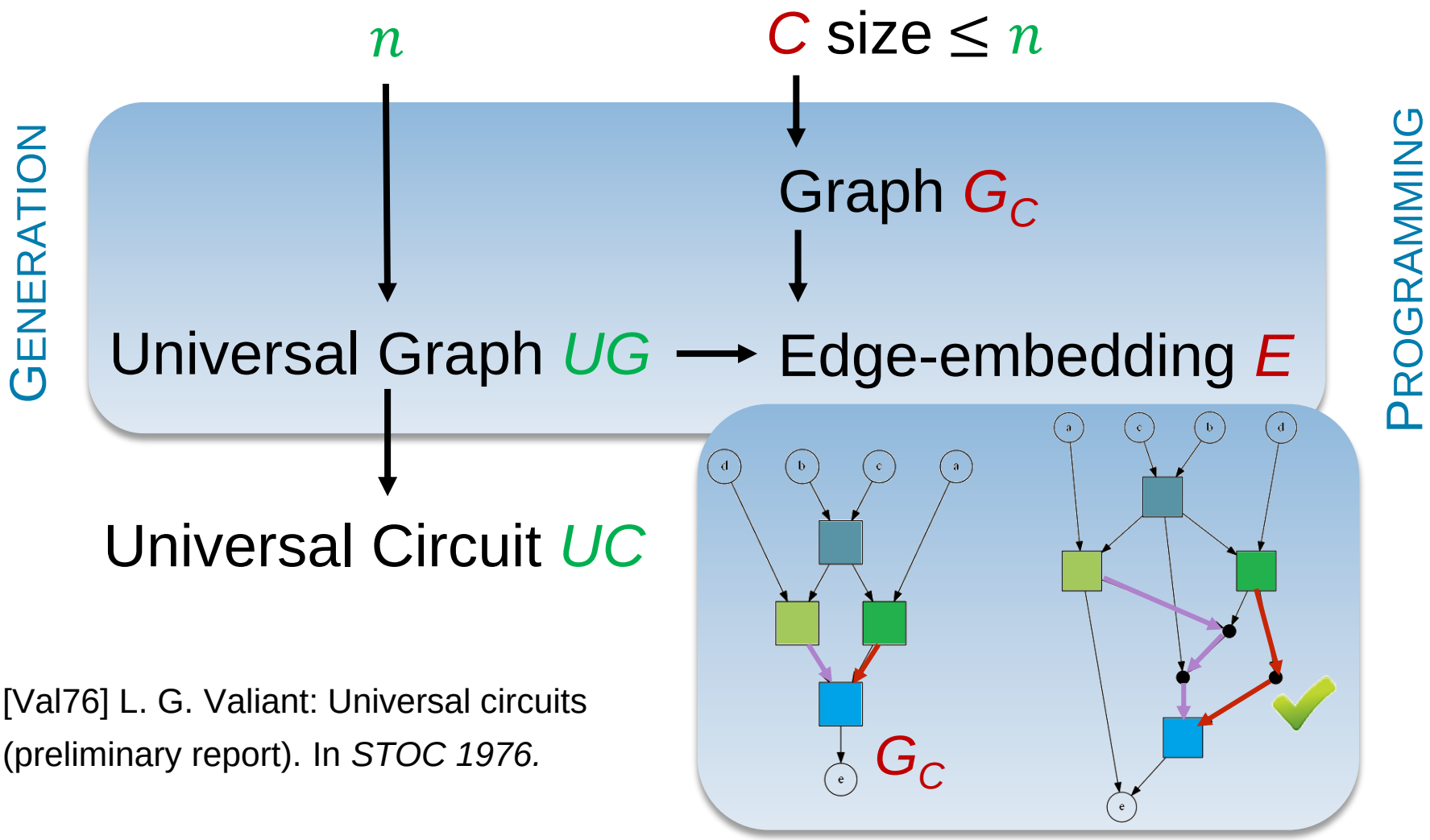
[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Valiant's UC Construction



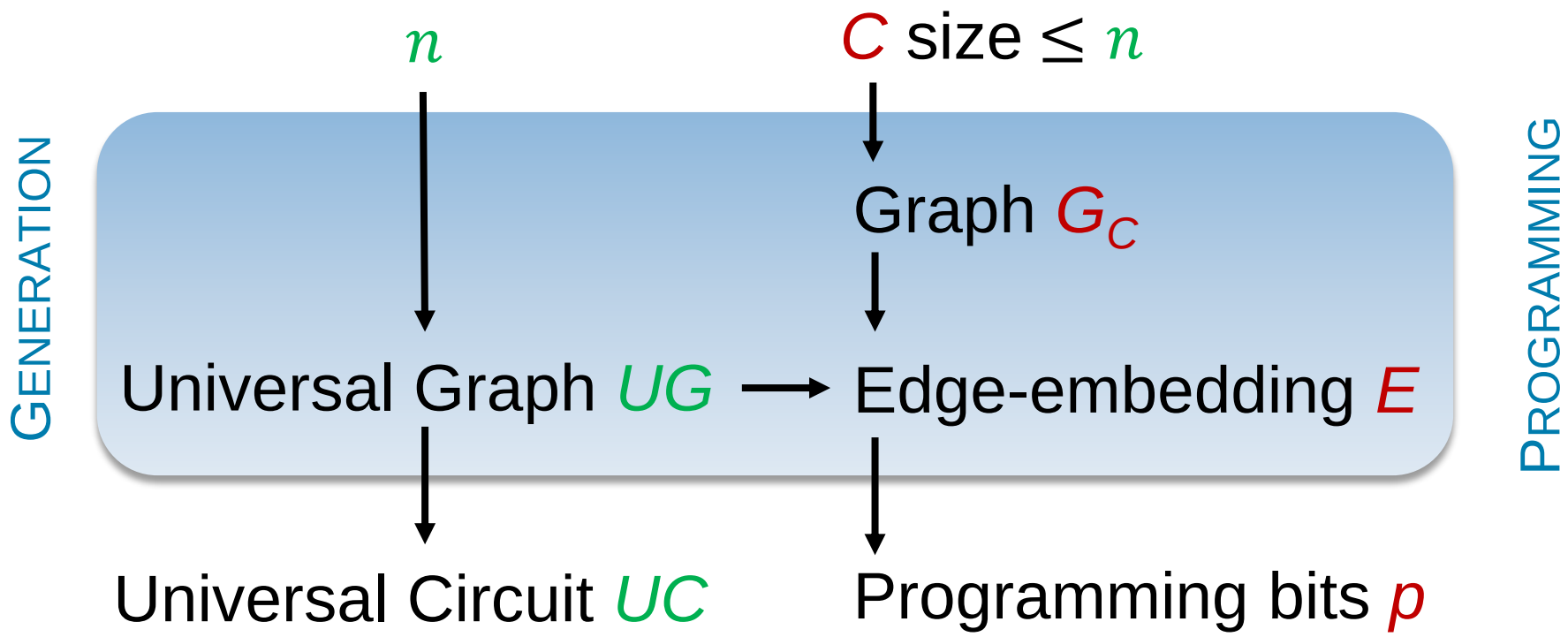
[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Valiant's UC Construction



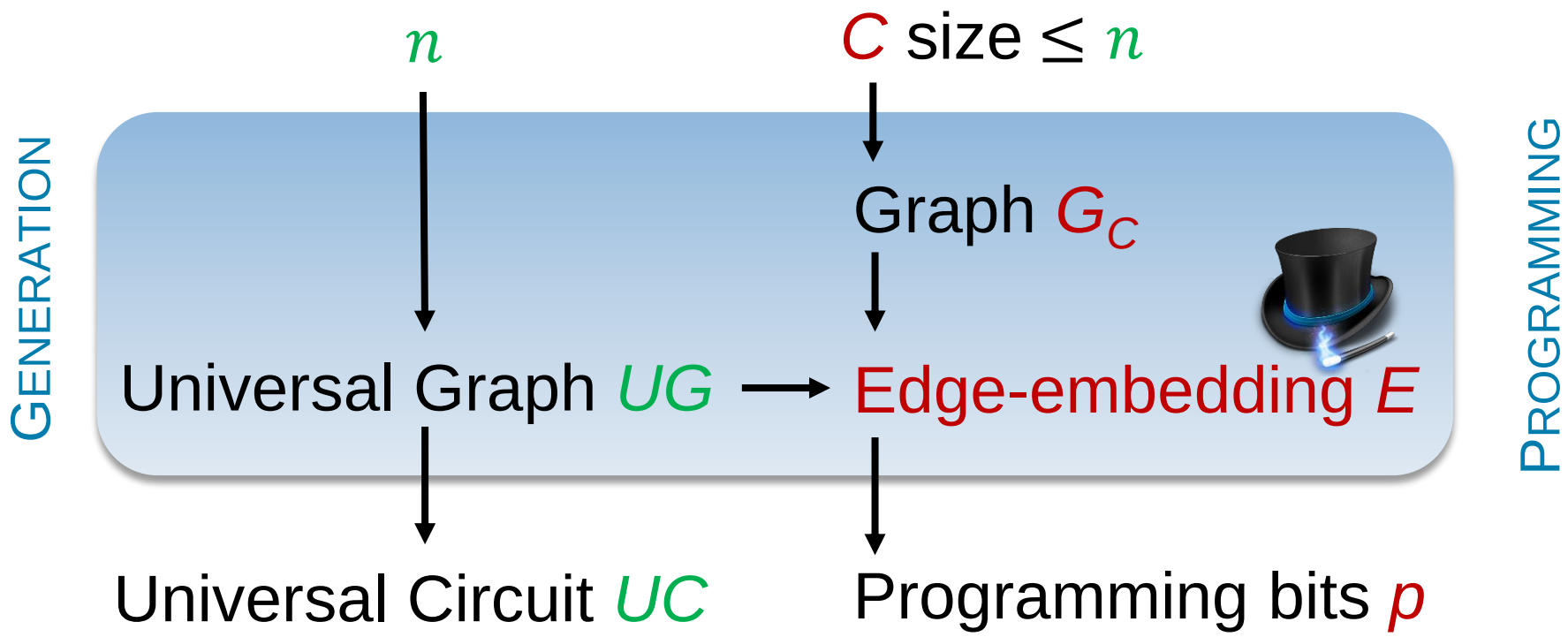
[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Valiant's UC Construction



[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

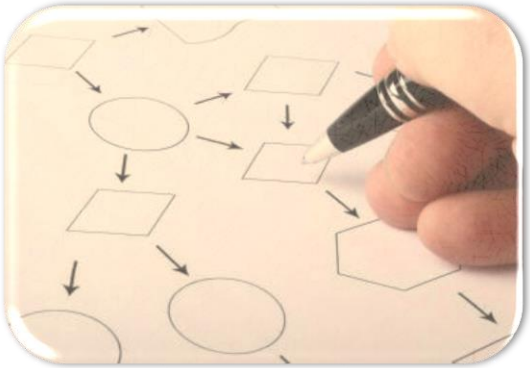
Valiant's UC Construction



[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

Our Contributions

Valiant's universal circuit is practical.



Embedding algorithm

Refined size of construction

UC compiler

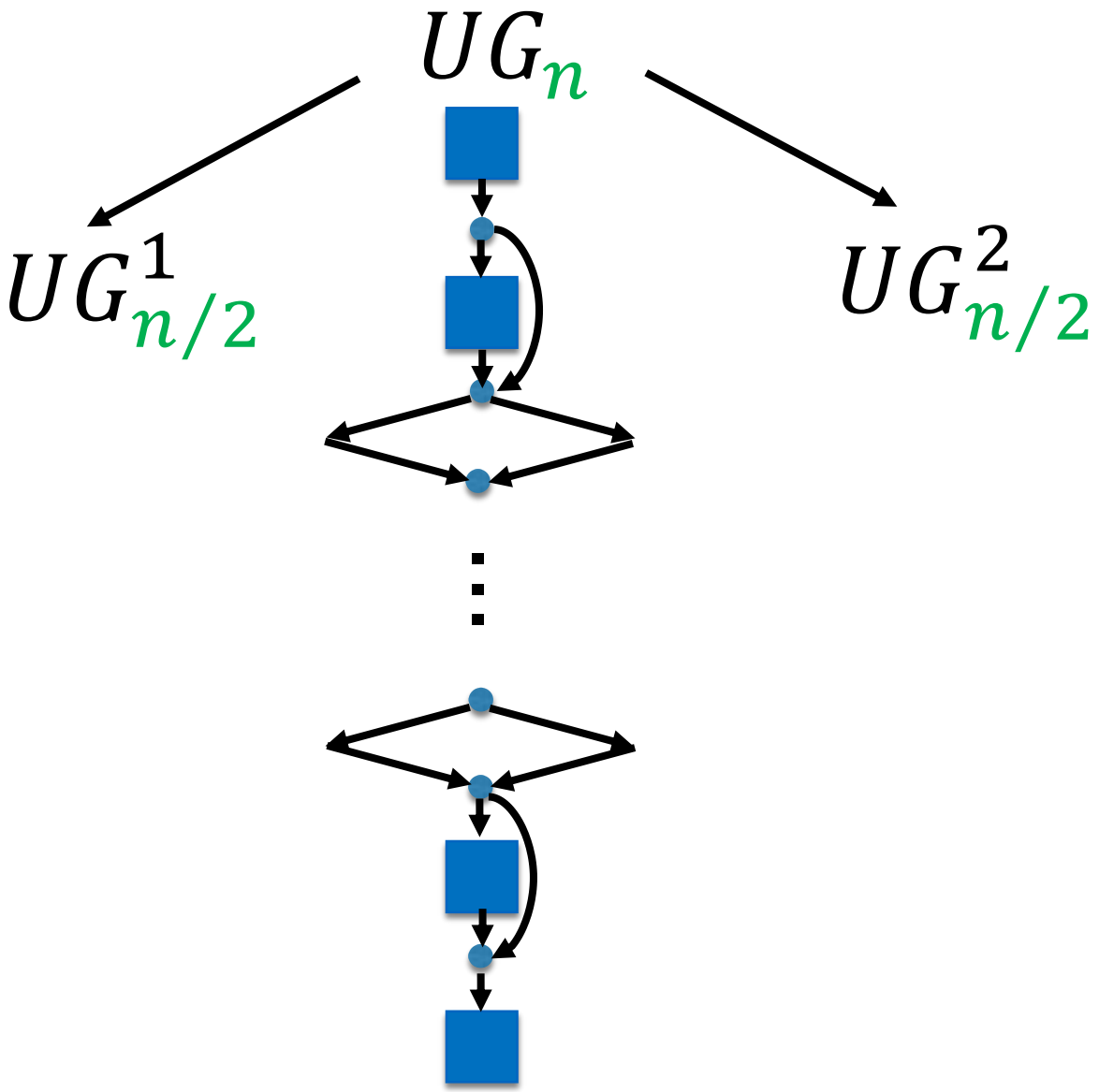
UG Embedding Algorithm

Graph G_C

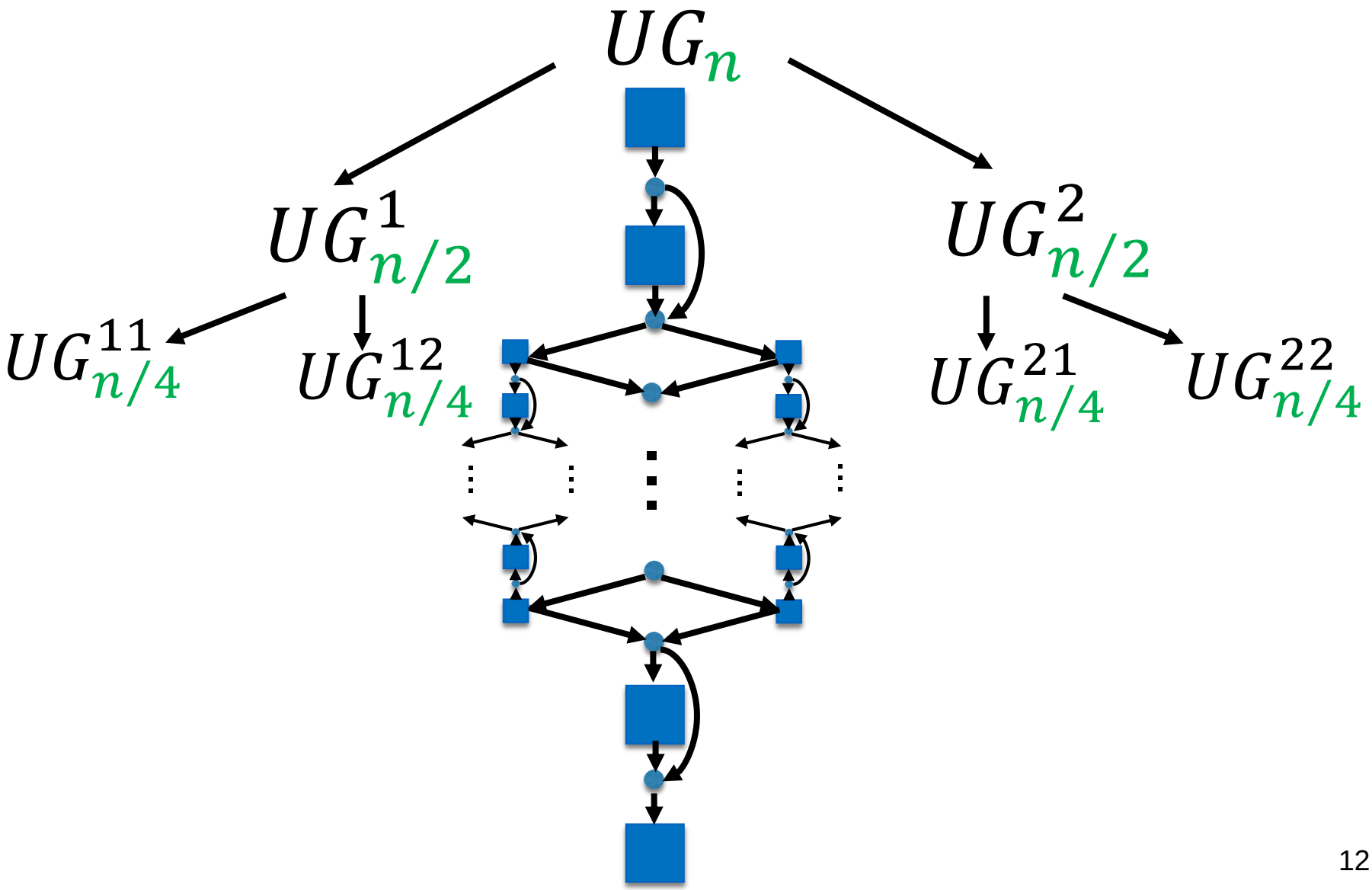
Universal Graph *UG* → Edge-embedding *E*

PROGRAMMING

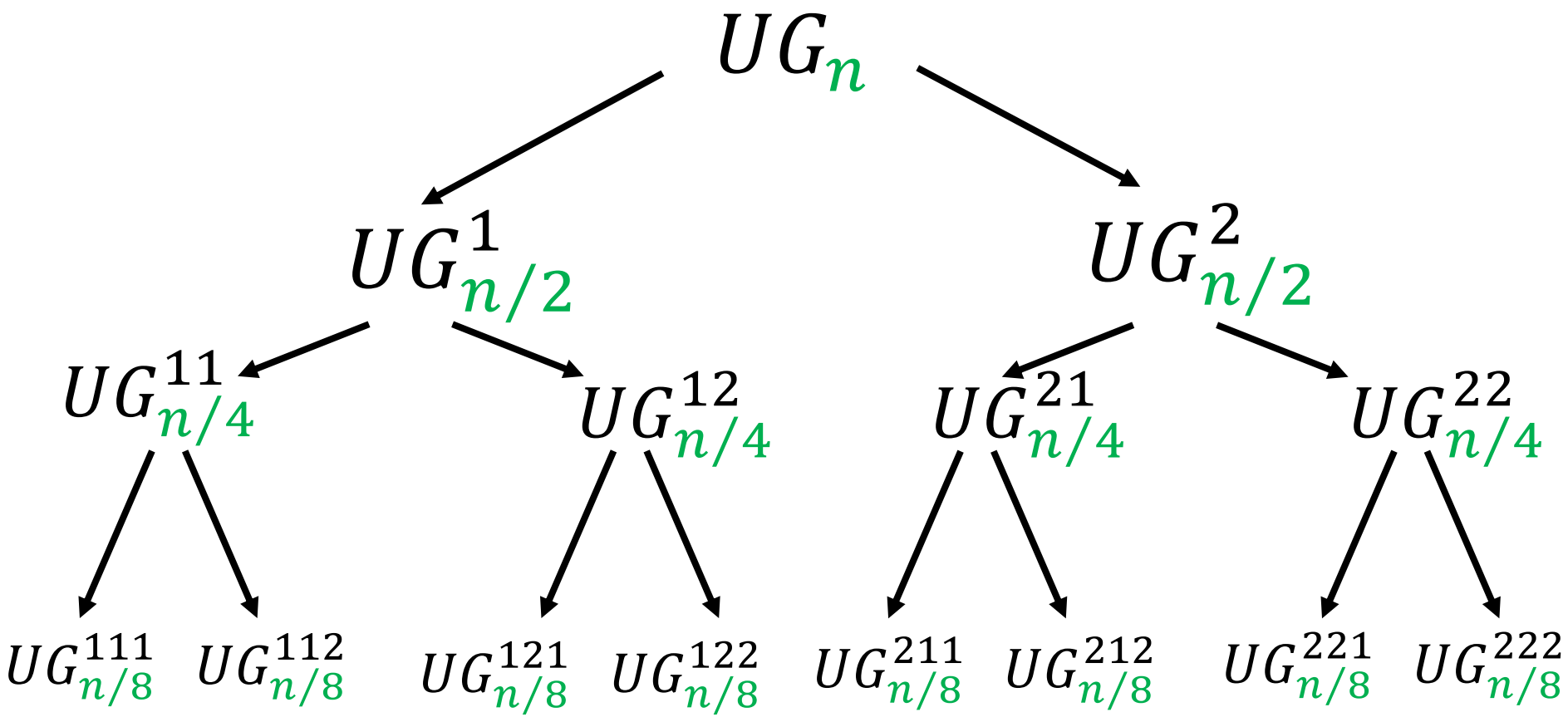
Recursive UG Construction



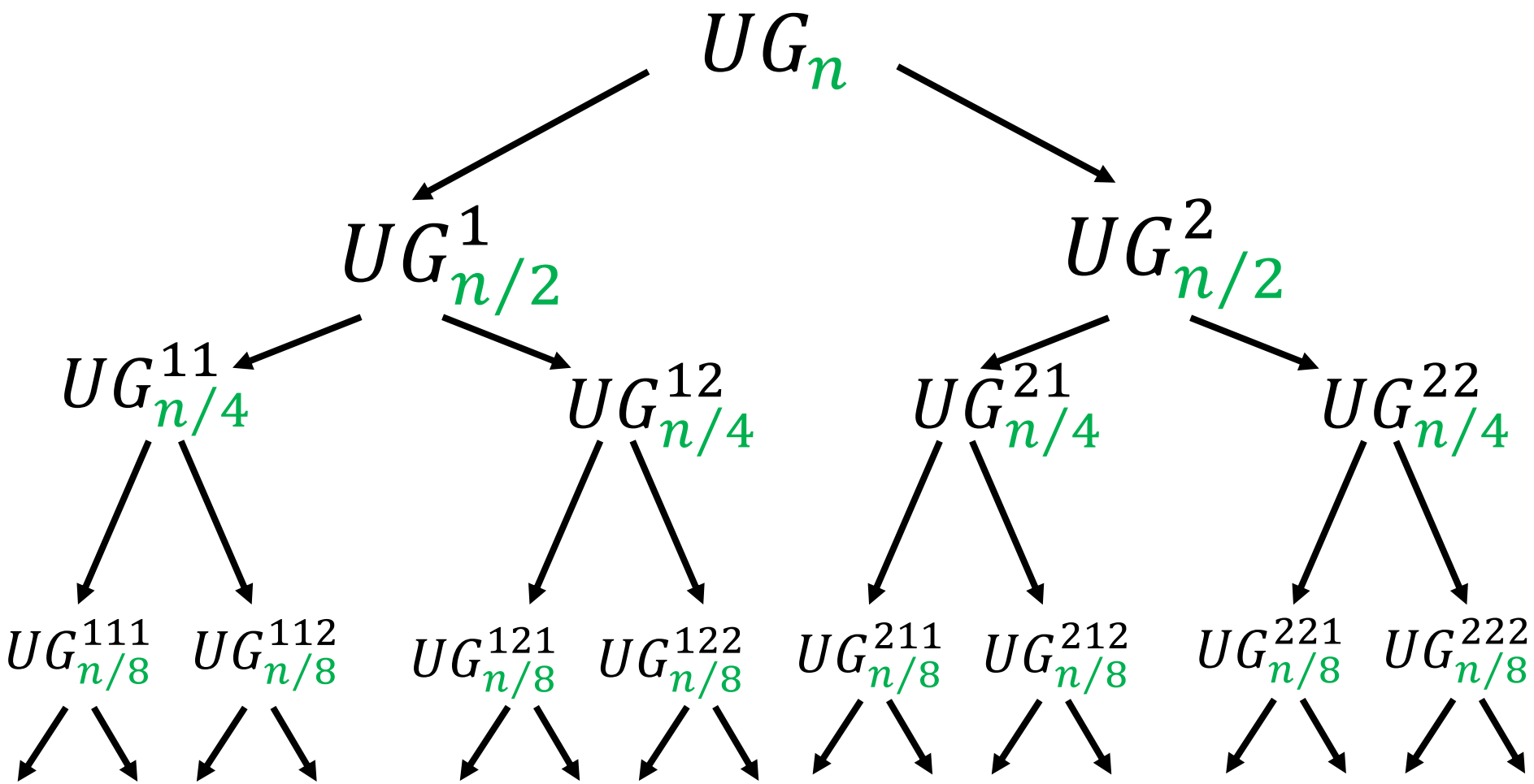
Recursive UG Construction



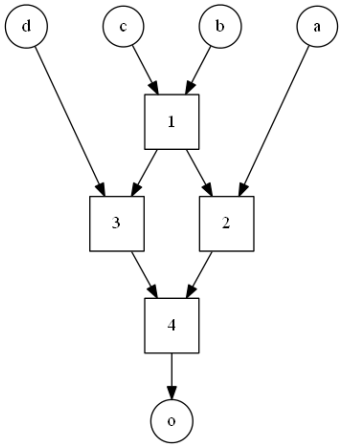
Recursive UG Construction



Recursive UG Construction

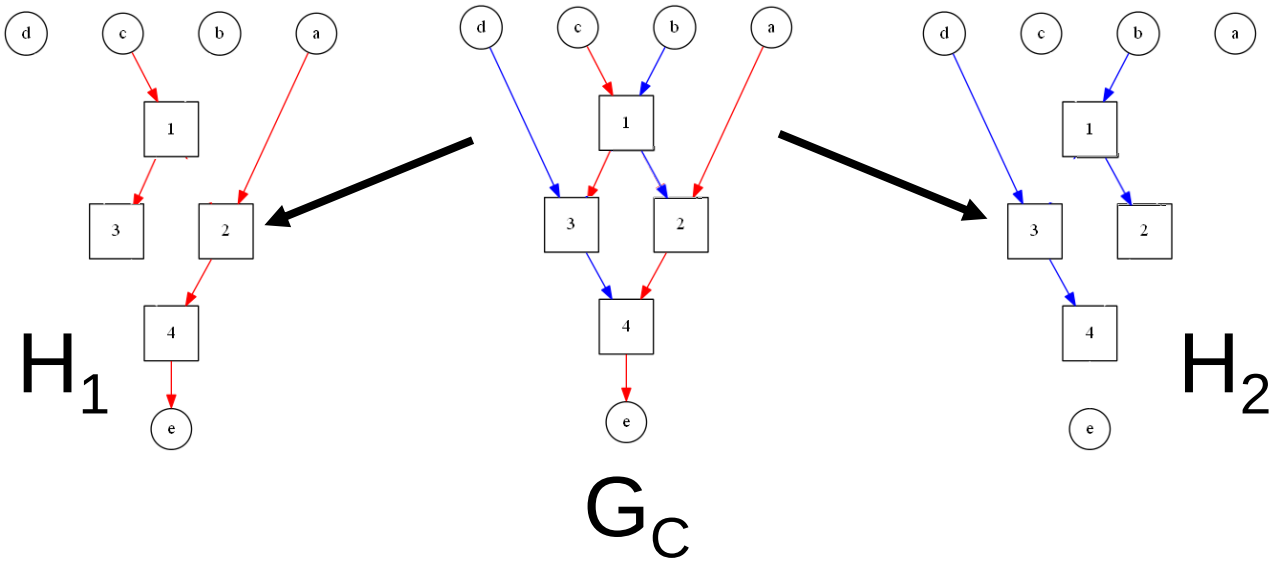


Edge-Embedding

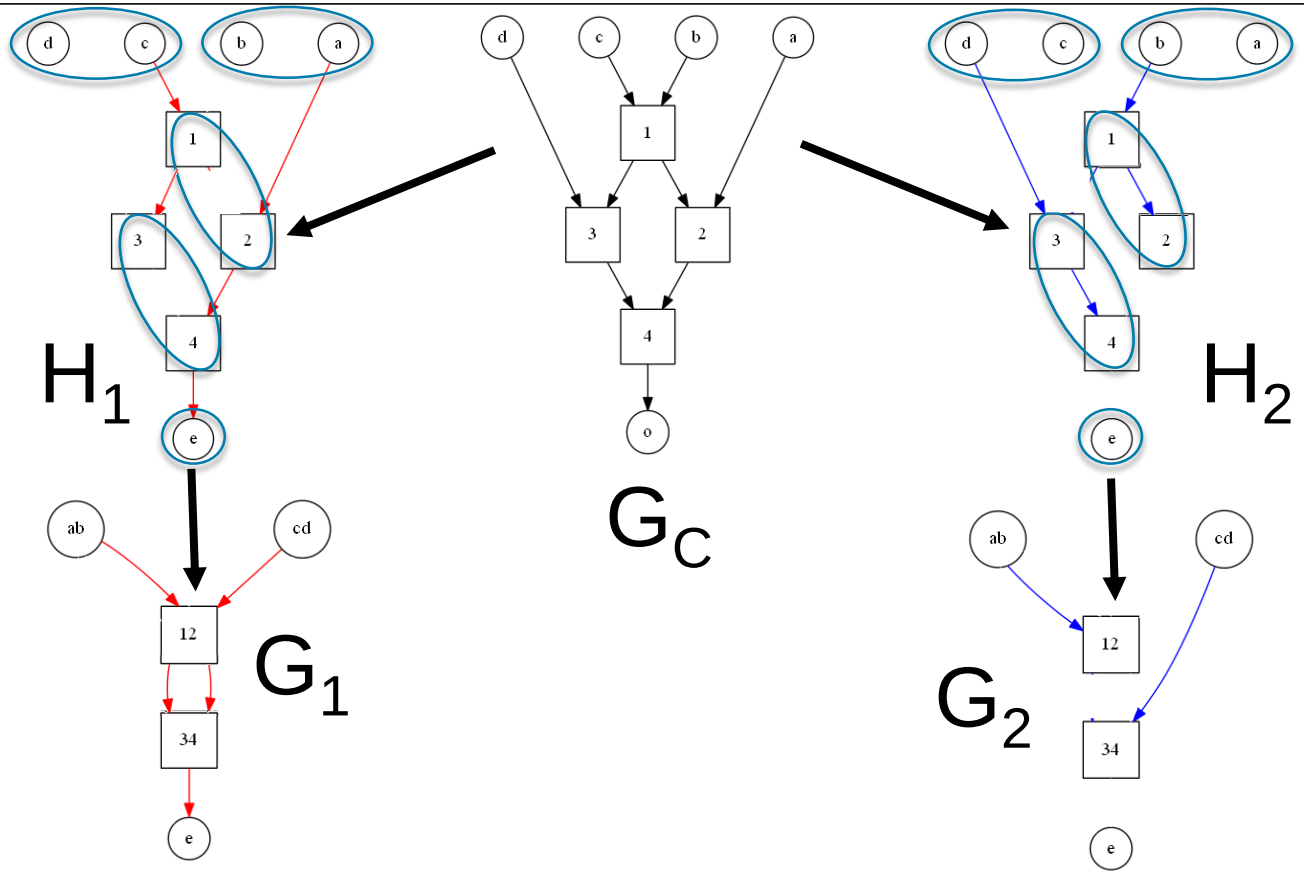


G_C

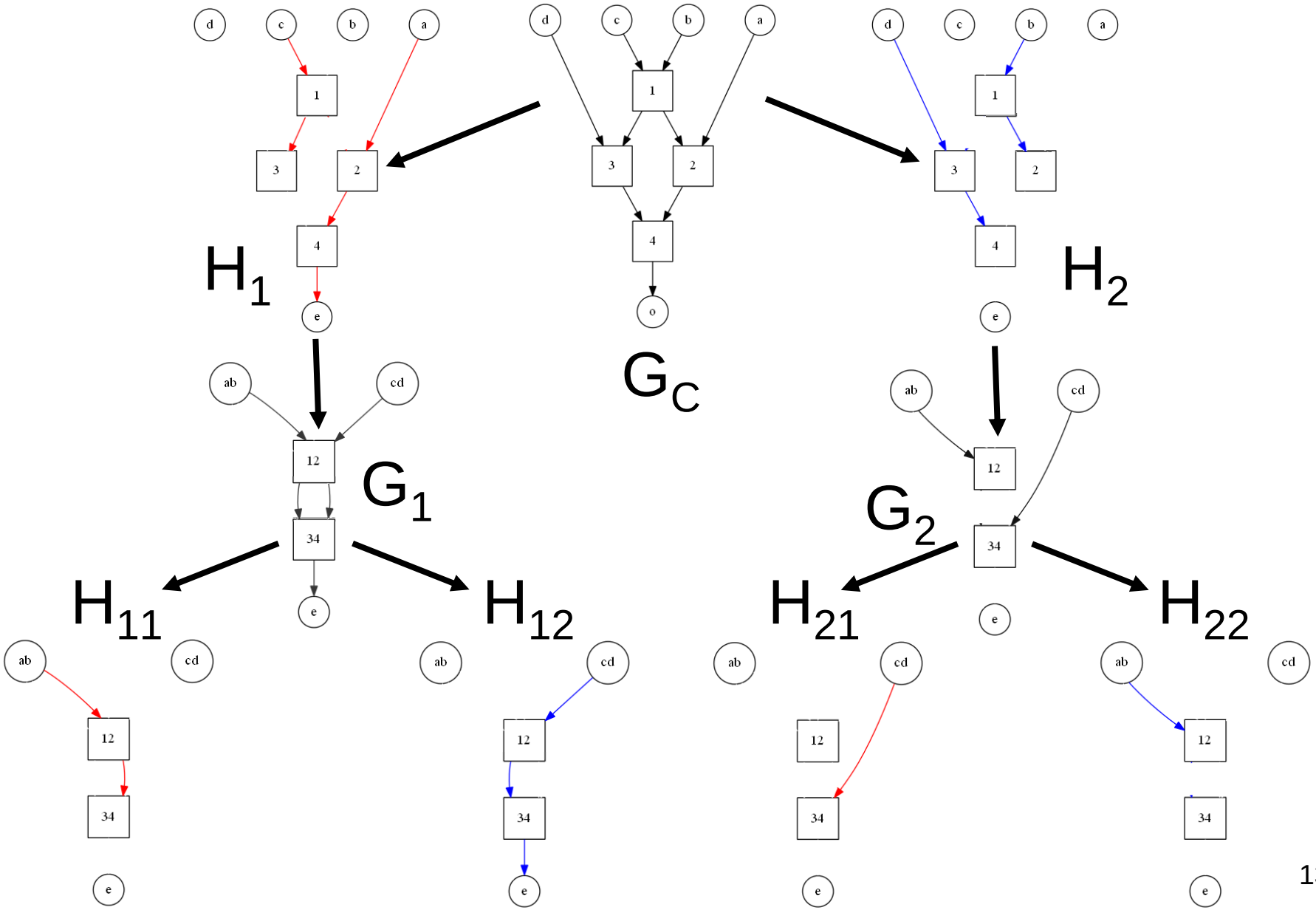
Edge-Embedding



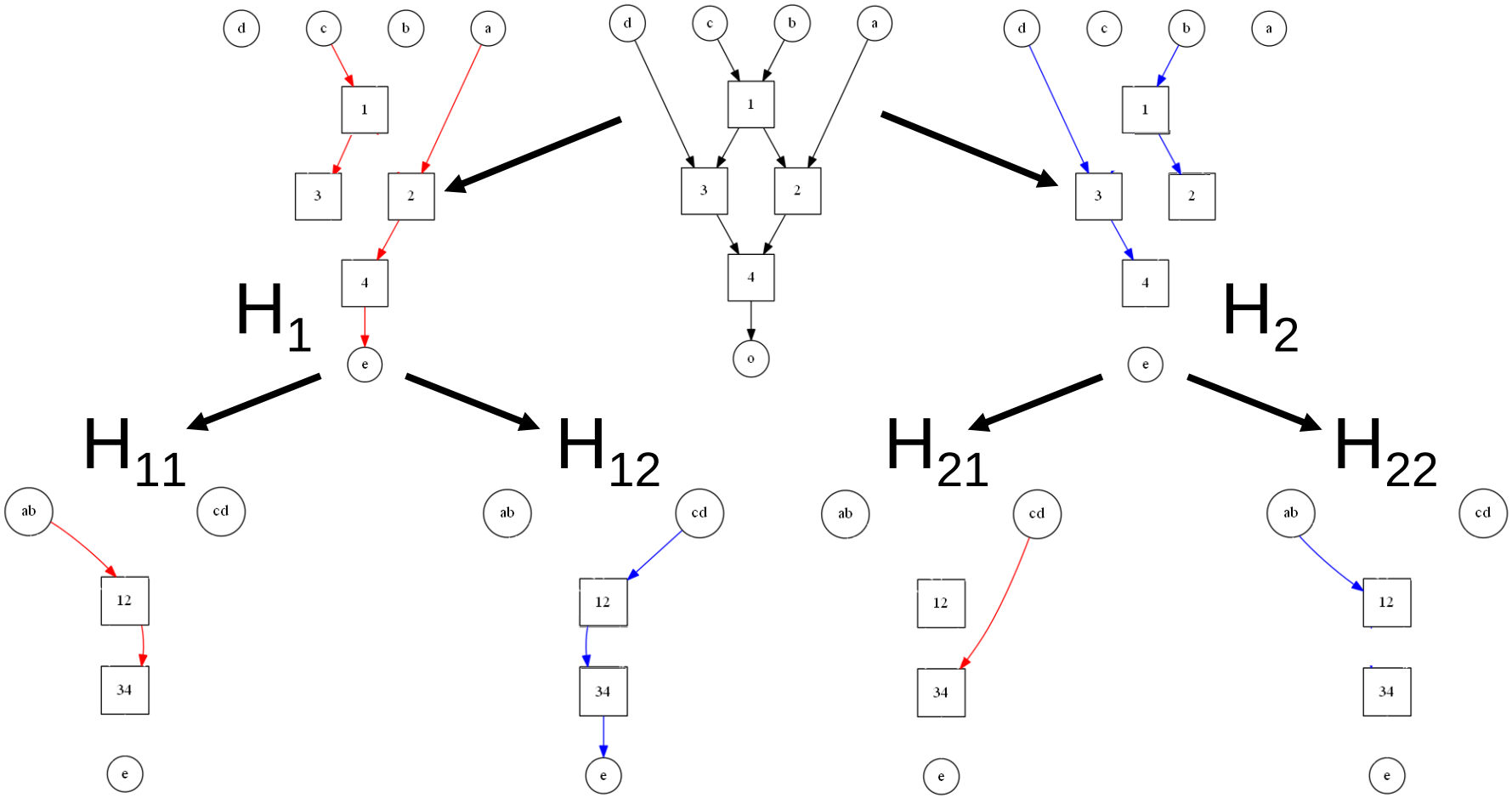
Edge-Embedding



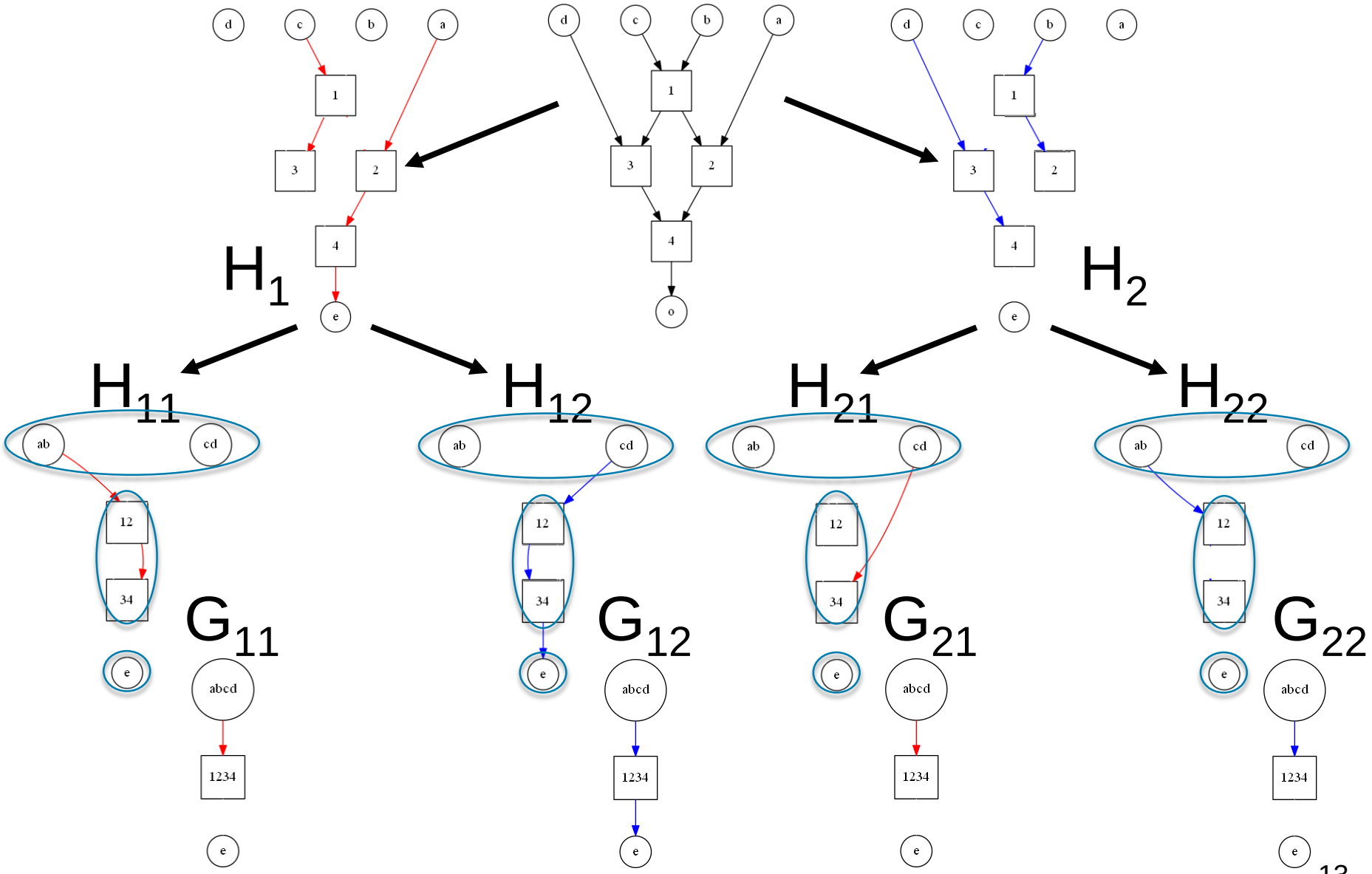
Edge-Embedding



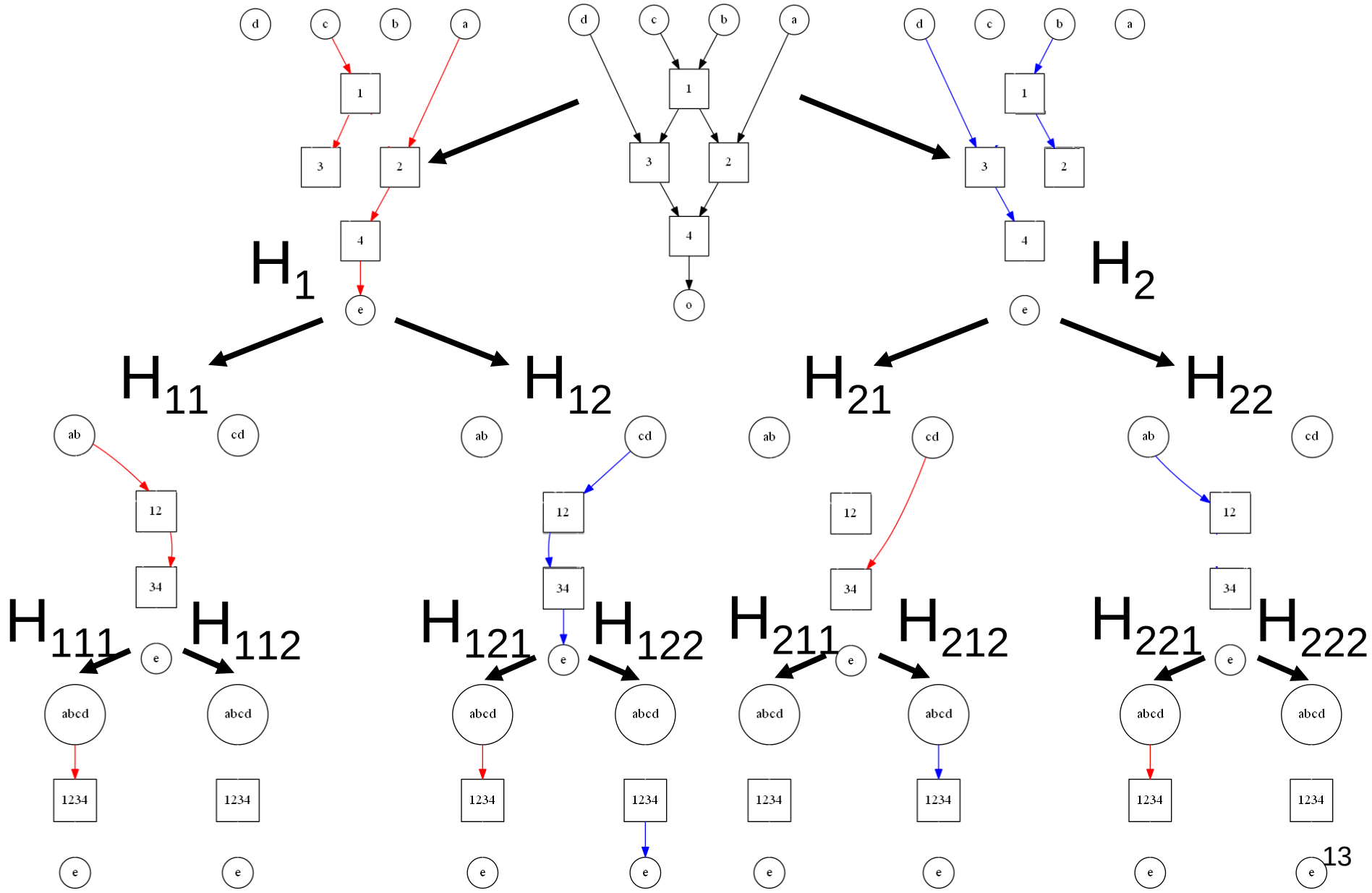
Edge-Embedding



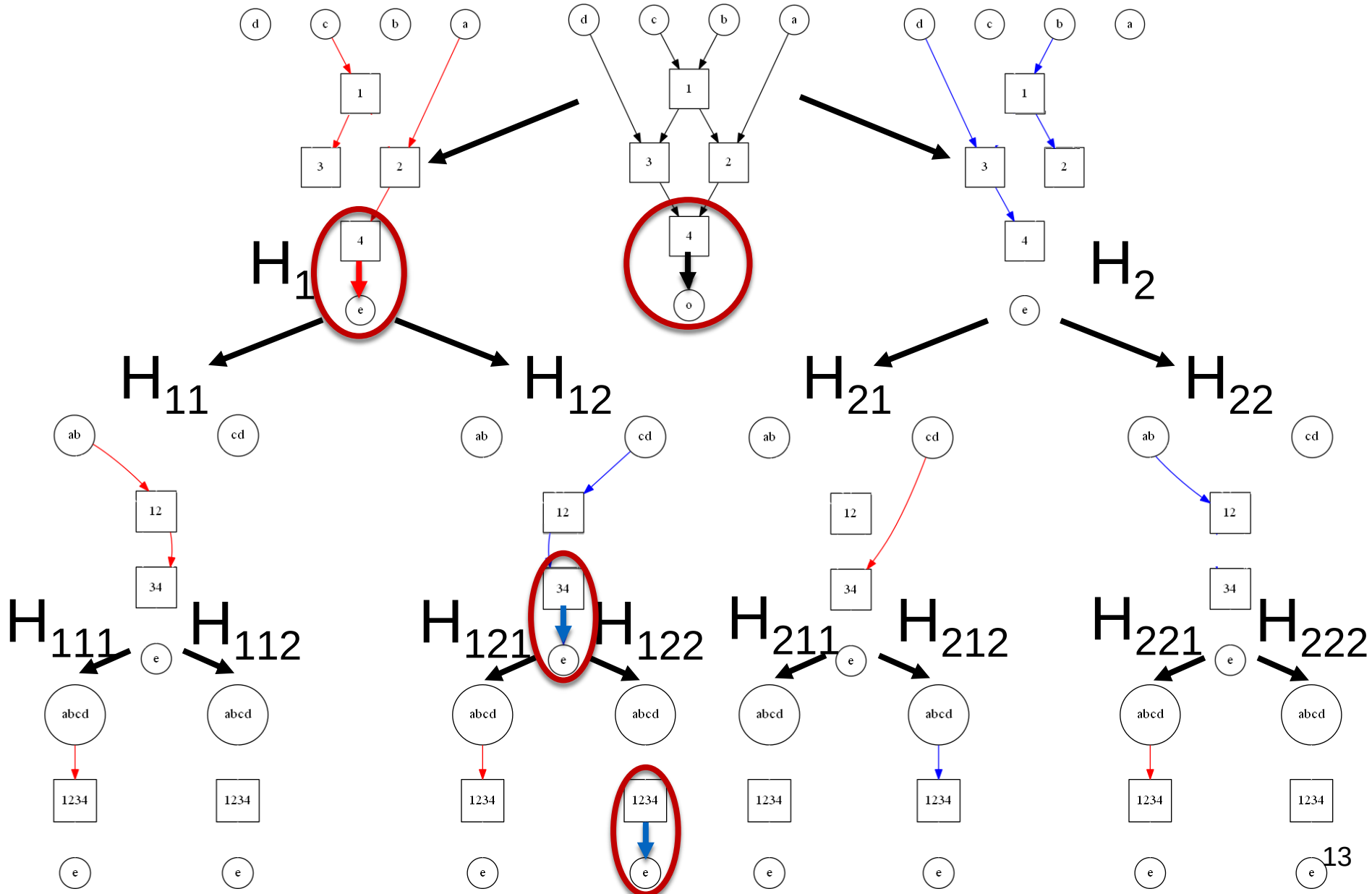
Edge-Embedding



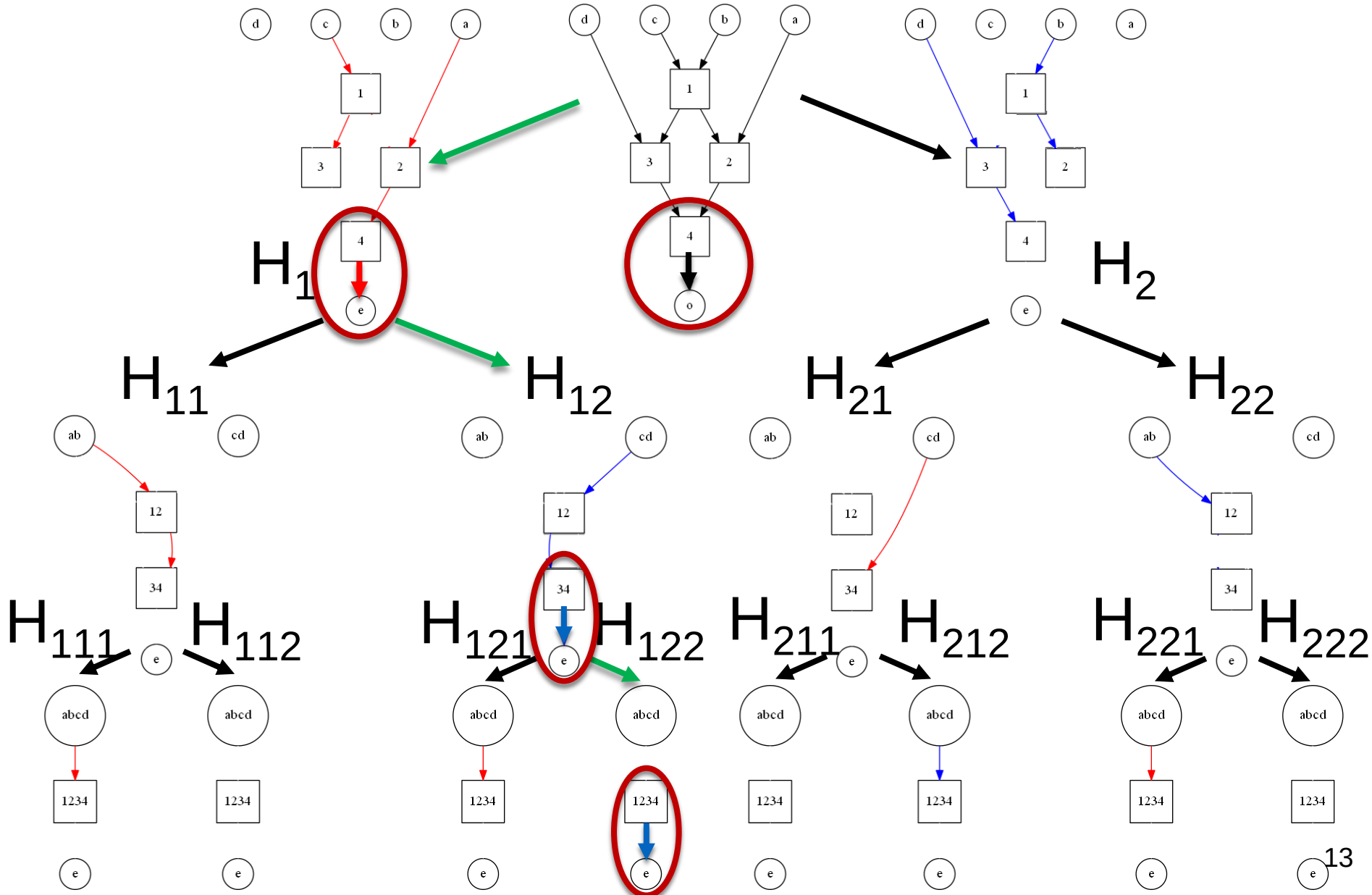
Edge-Embedding



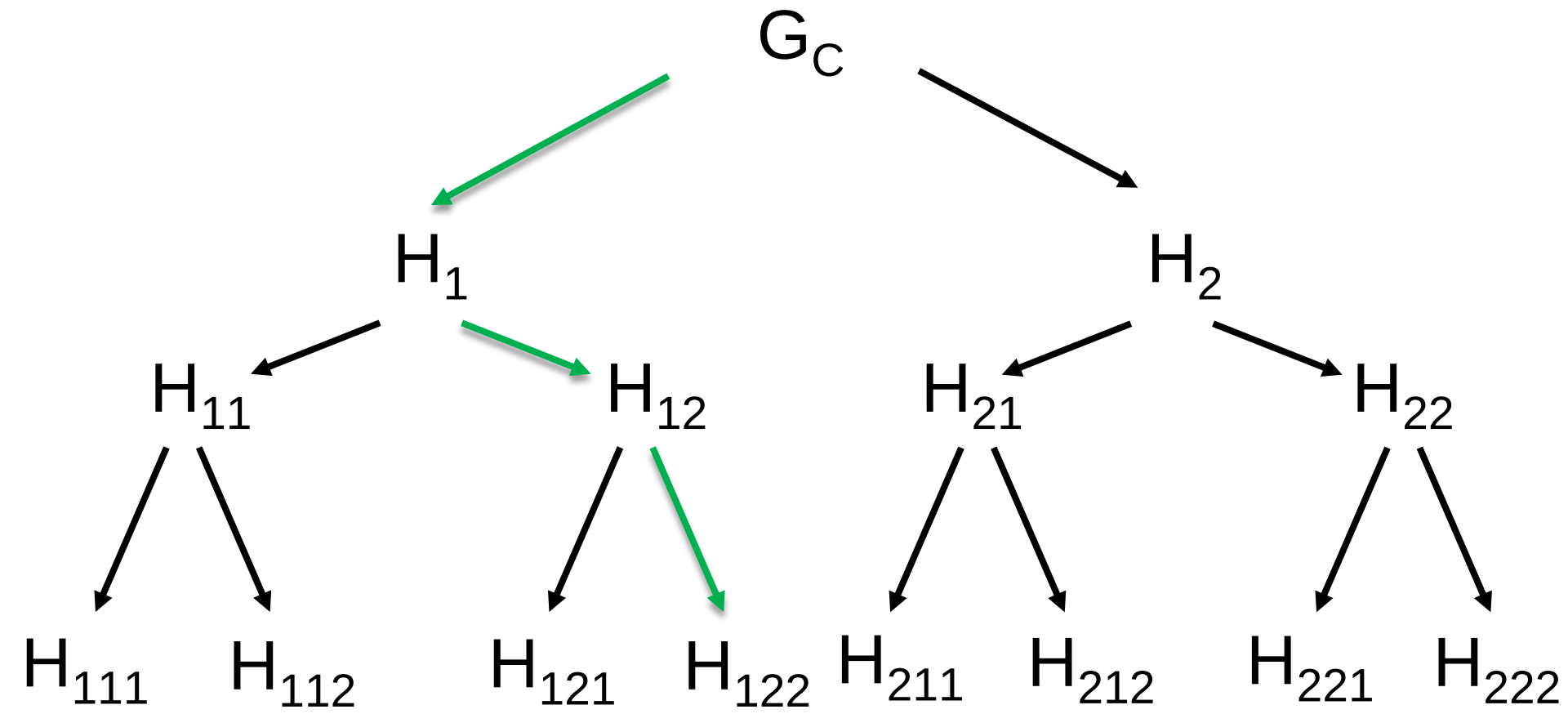
Edge-Embedding



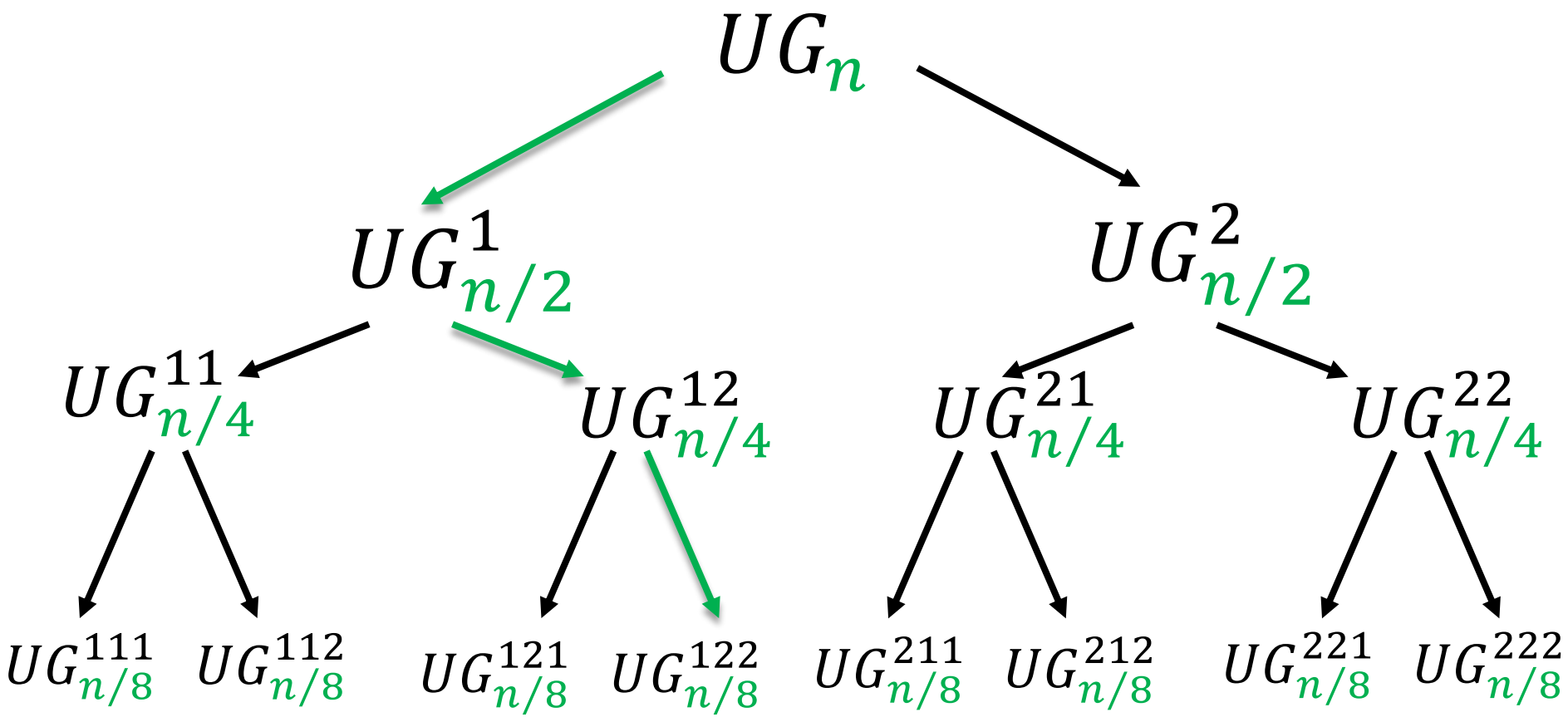
Edge-Embedding



Edge-Embedding



Recursive UG Construction



Our Contributions

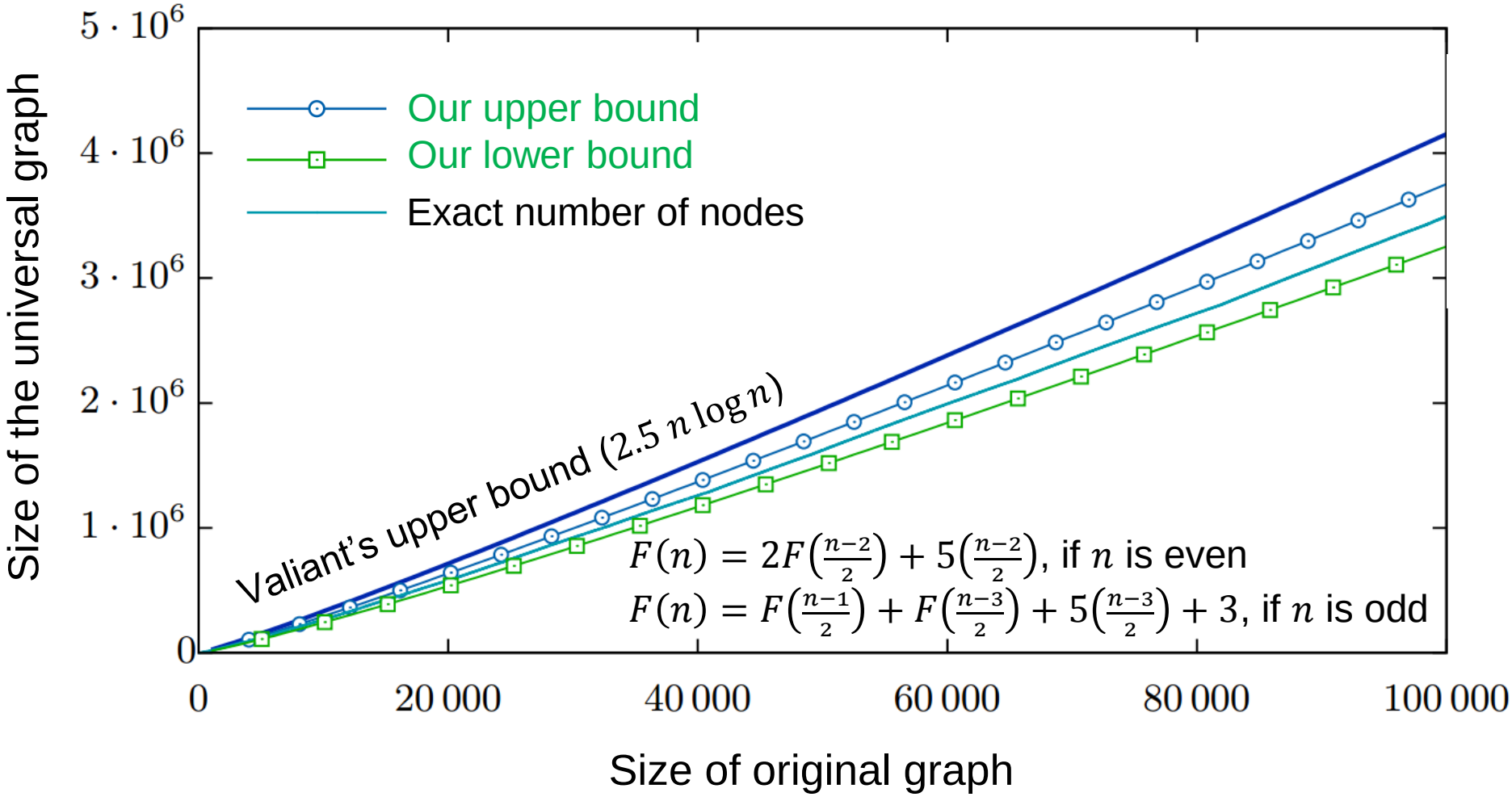
Valiant's universal circuit is practical.

Embedding algorithm

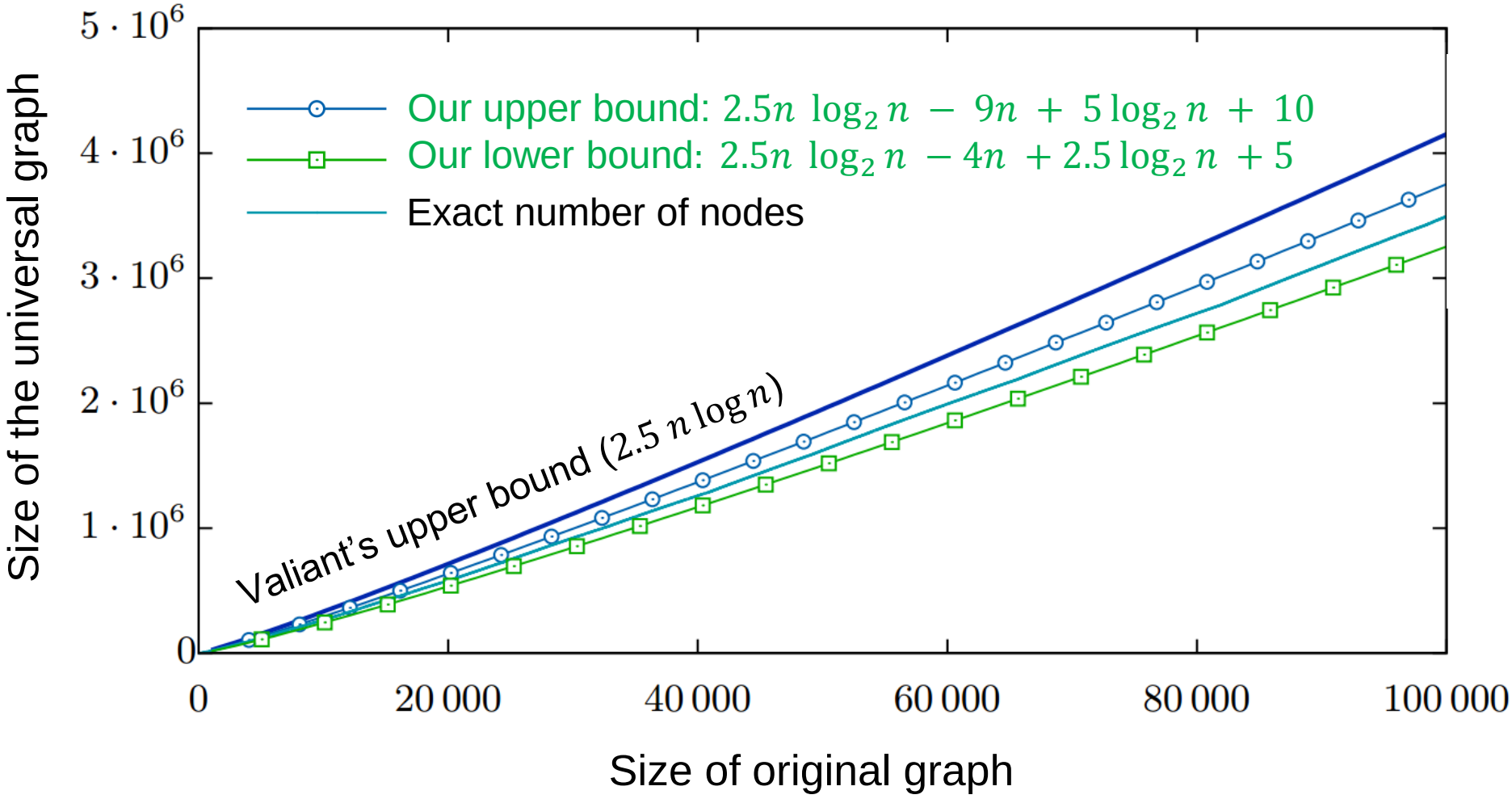
Refined size of construction

UC compiler

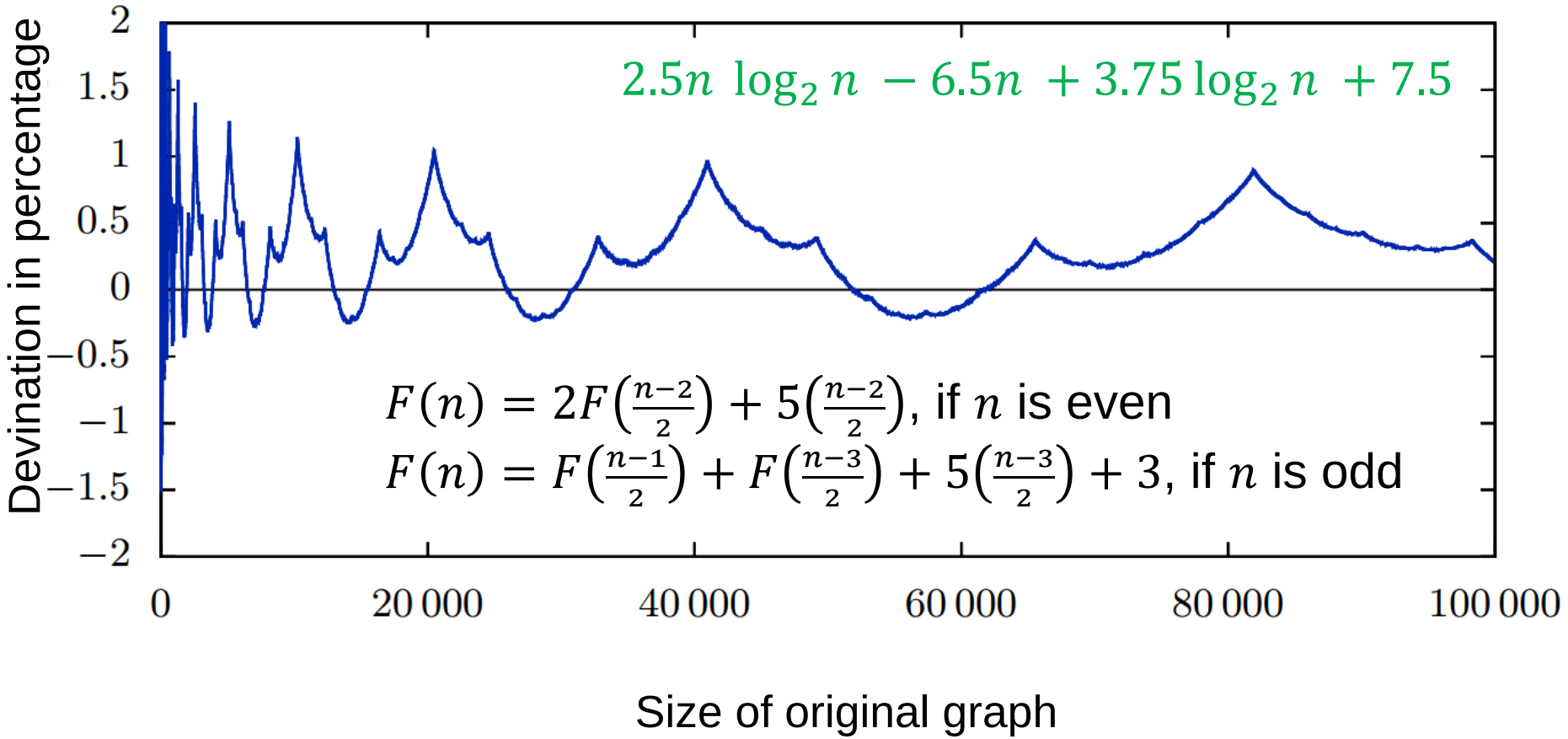
Size of Universal Graph



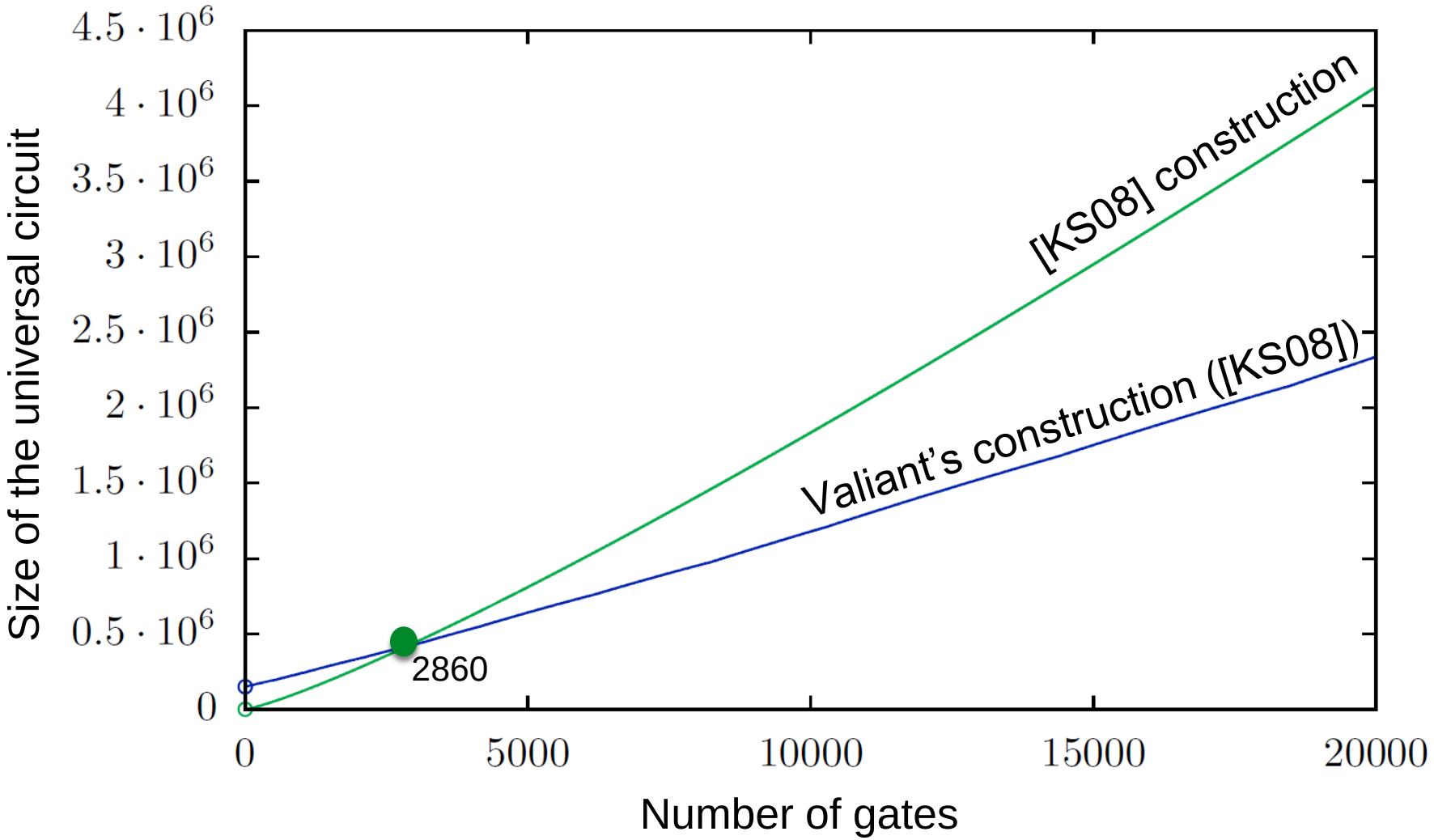
Size of Universal Graph



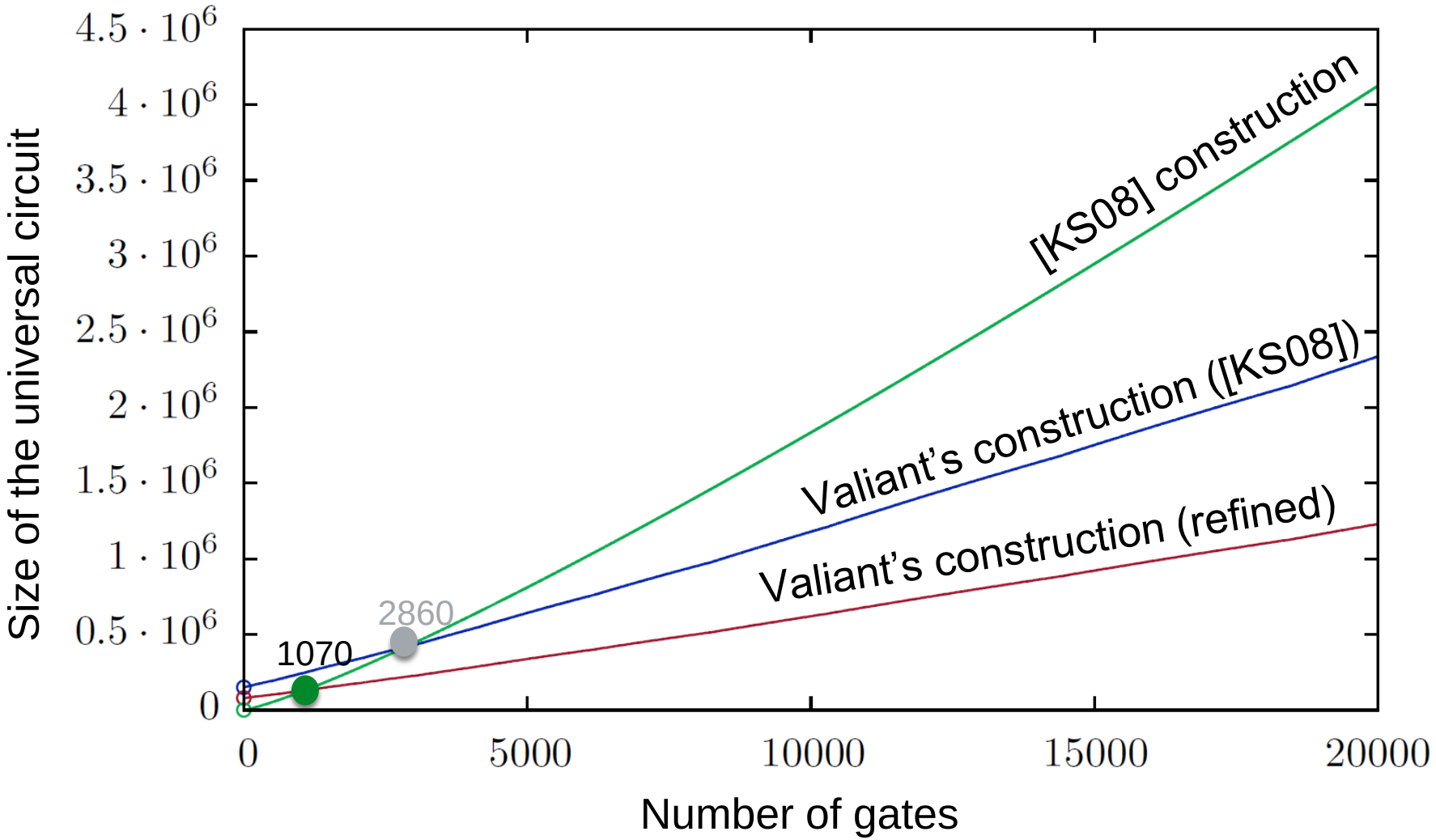
Deviation of Estimated Size and Exact Size



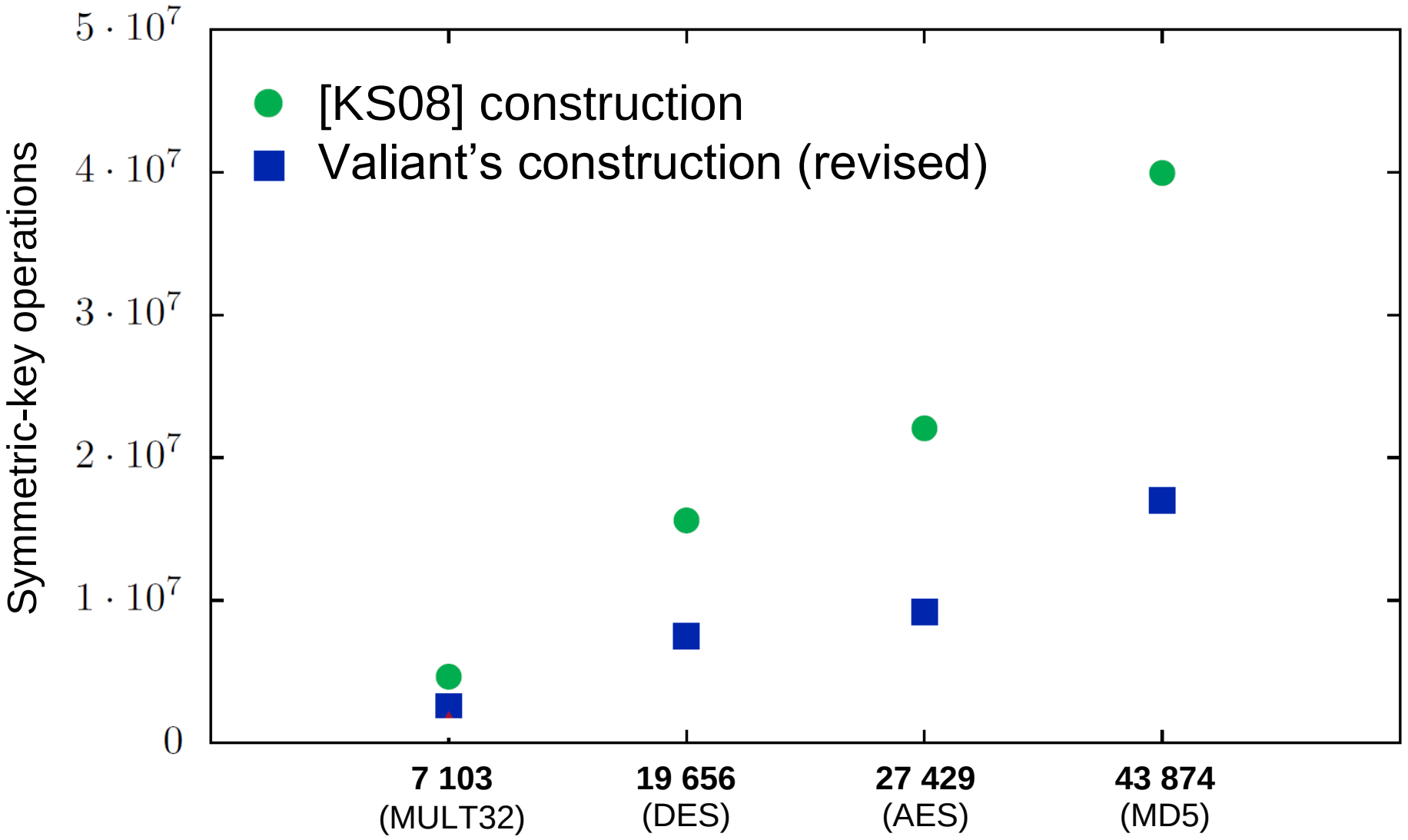
Size of the UC Constructions [KS08]



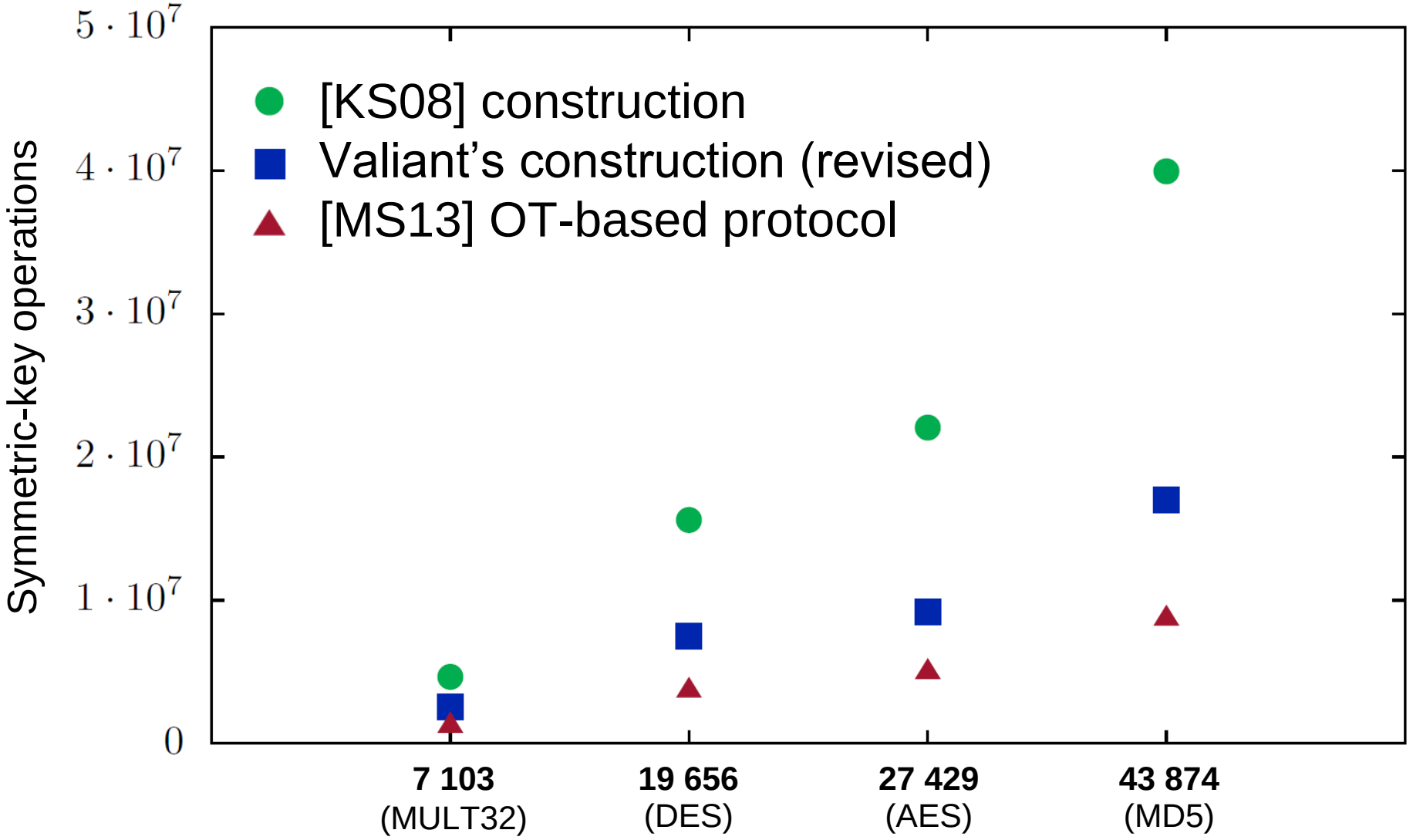
Revised size of the UC Constructions



PFE Comparison – Symmetric-Key Operations



PFE Comparison – Symmetric-Key Operations



[MS13]: P. Mohassel, S. S. Sadeghian. How to hide circuits in MPC an efficient framework for private function evaluation. In *Eurocrypt 2013*.

Our Contributions

Valiant's universal circuit is practical.

Embedding algorithm

Refined size of construction

UC compiler

UC Implementation

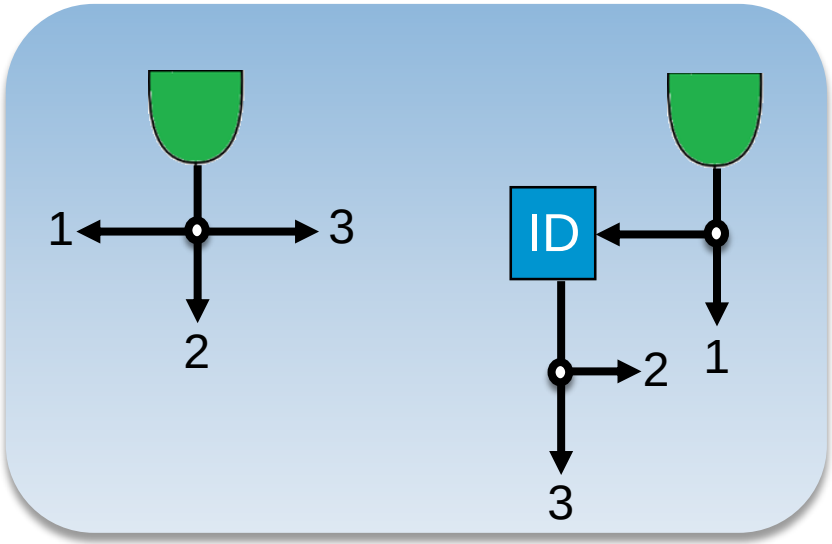
SHDL

$C_0 \longleftarrow f$

[MNPS04] D. Malkhi, N. Nisan, B. Pinkas, Y. Sella. Fairplay-Secure Two-Party Computation System. In *USENIX Security Symposium* 2004.

UC Implementation

C size $\leq n \longleftarrow C_0 \longleftarrow f$

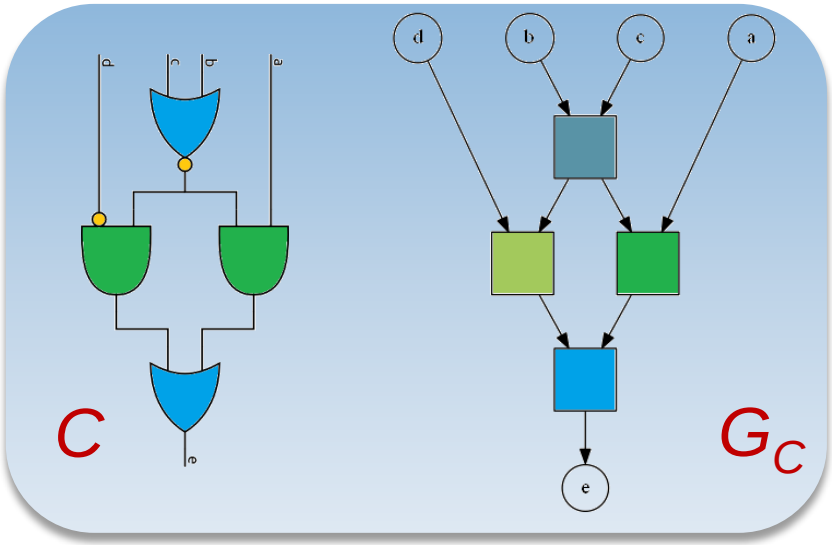


UC Implementation

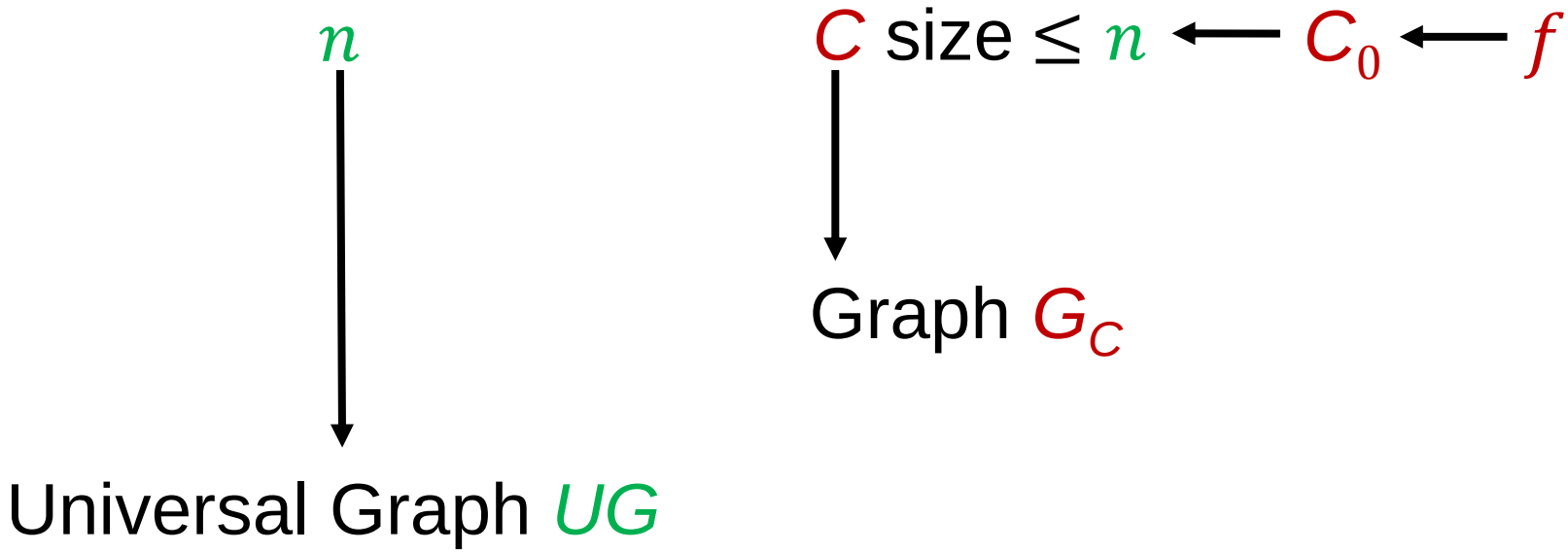
C size $\leq n \longleftarrow C_0 \longleftarrow f$

$\downarrow$

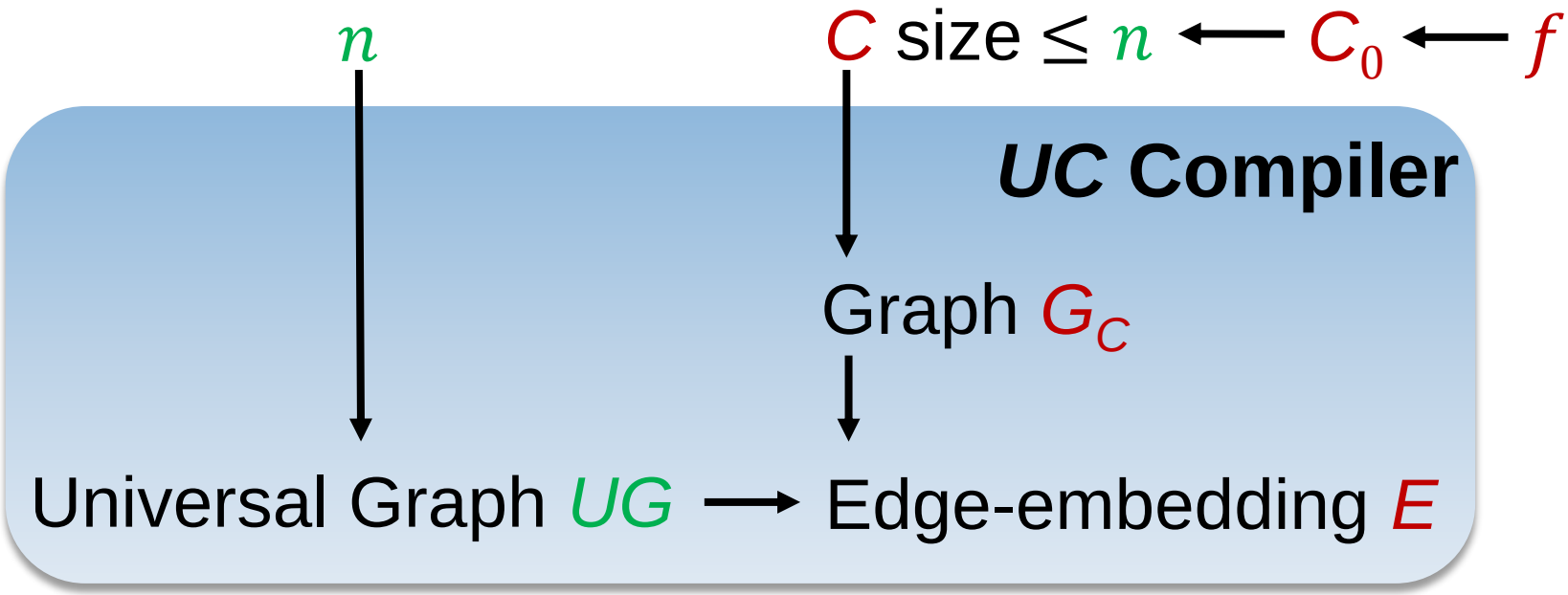
Graph G_C



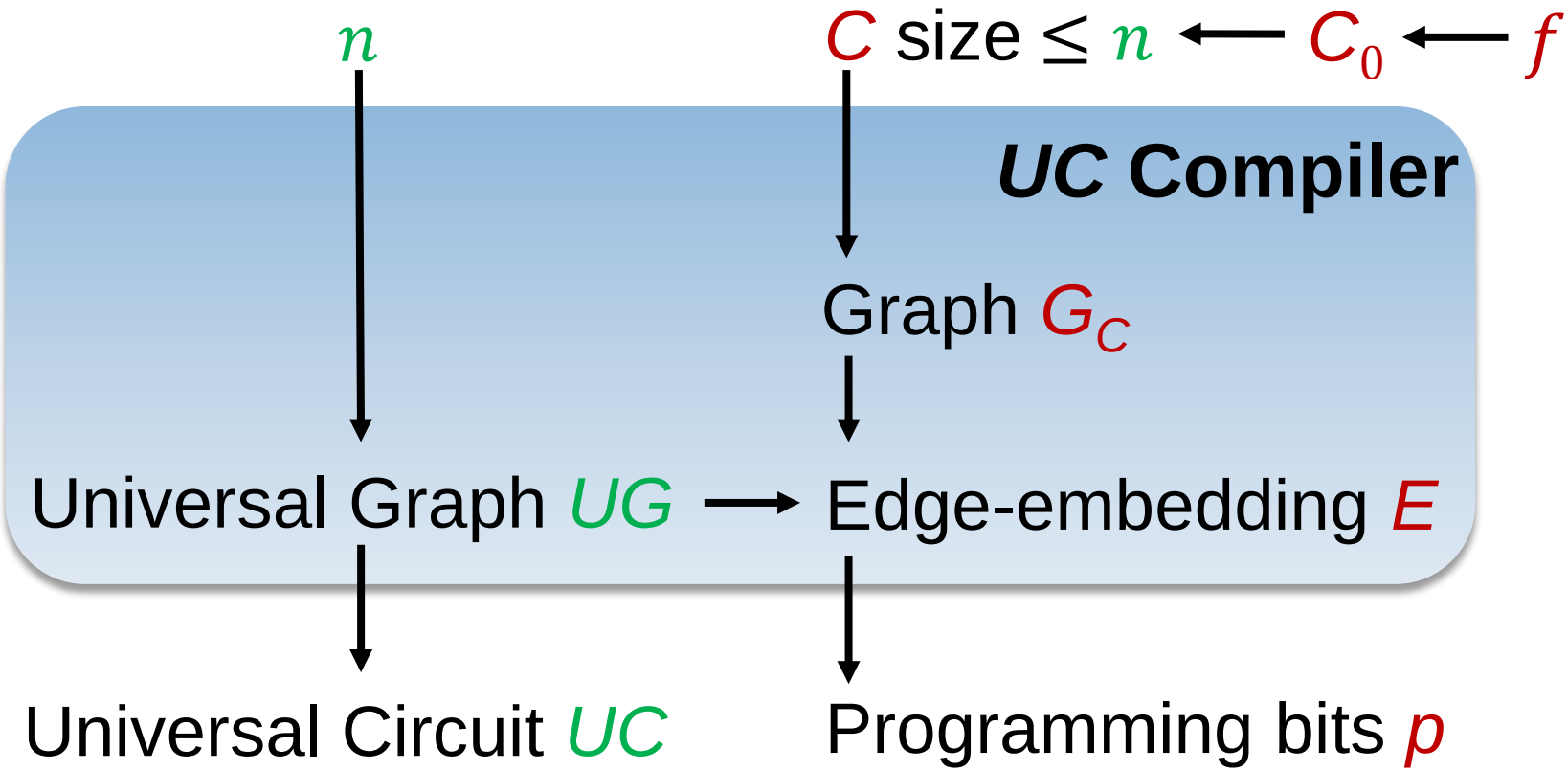
UC Implementation



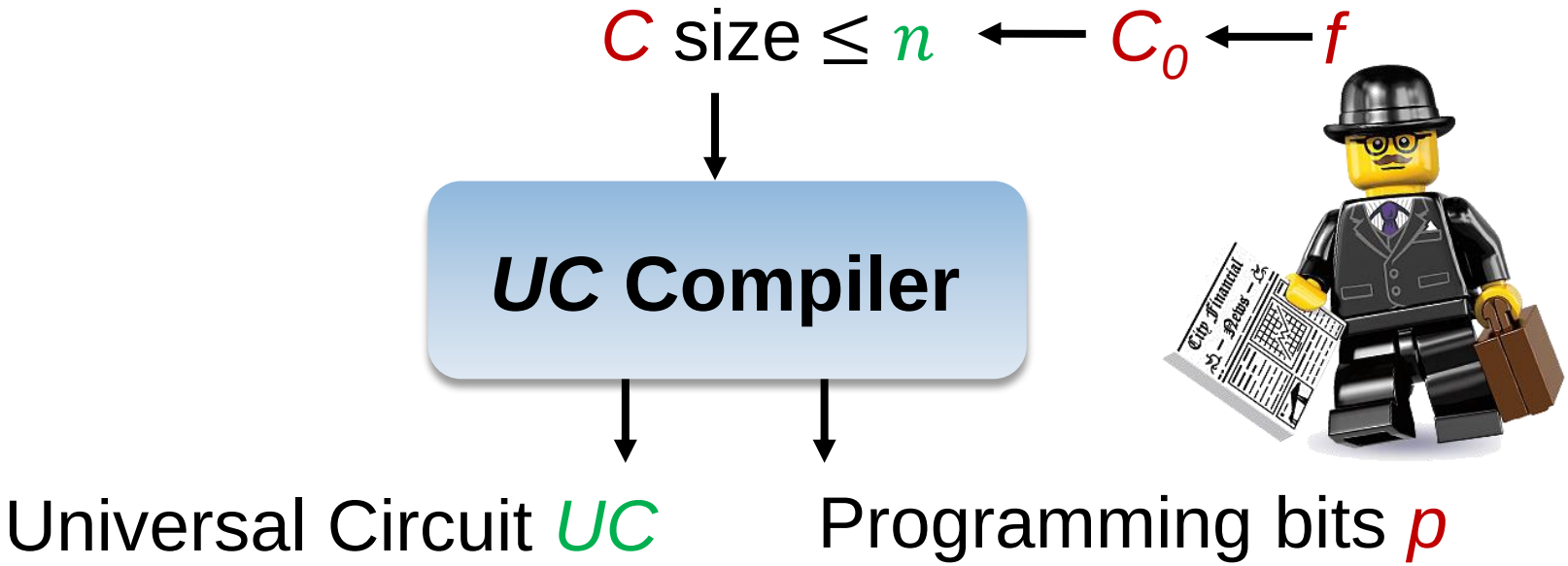
UC Implementation



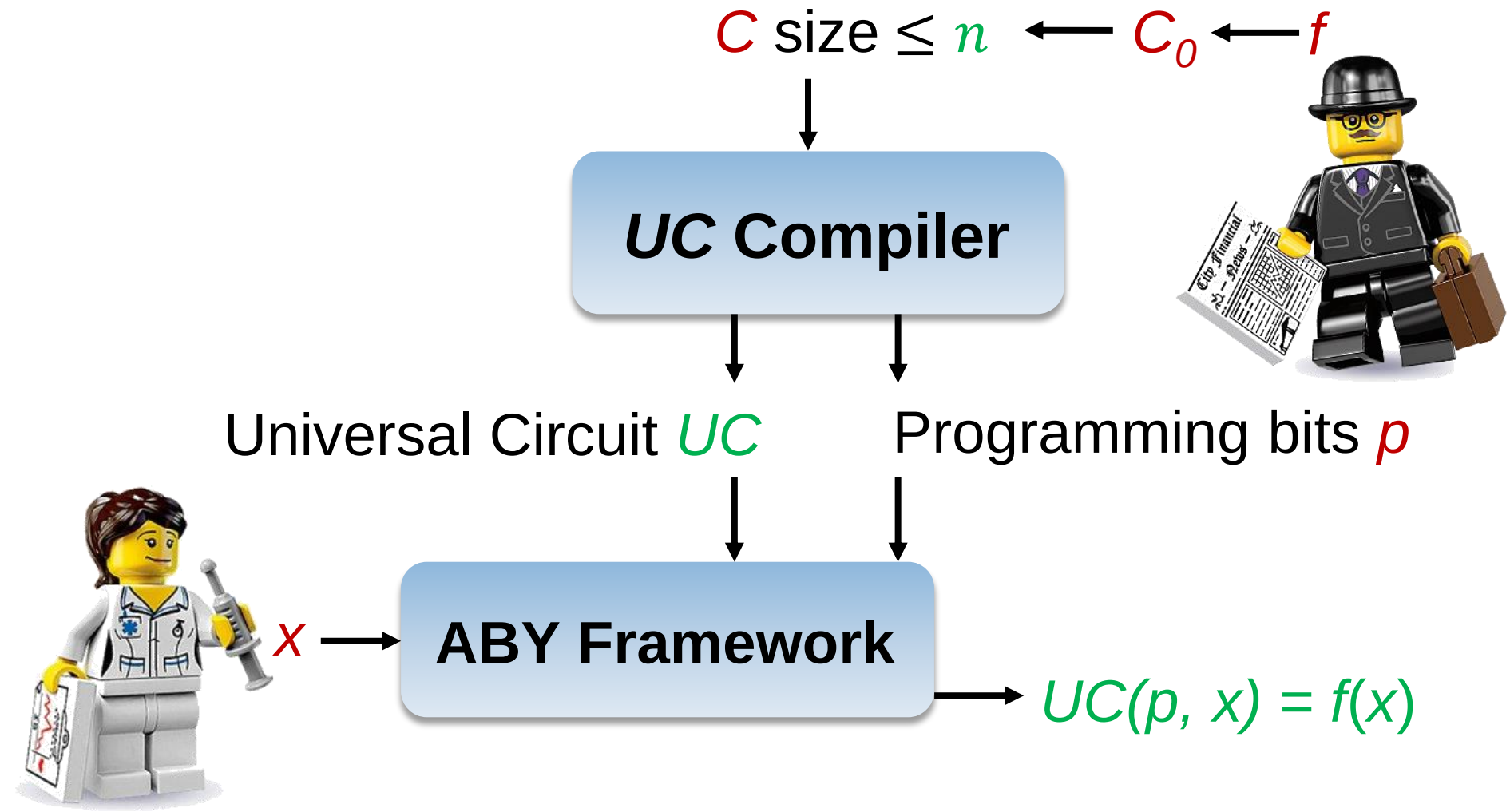
UC Implementation



PFE Implementation



PFE Implementation



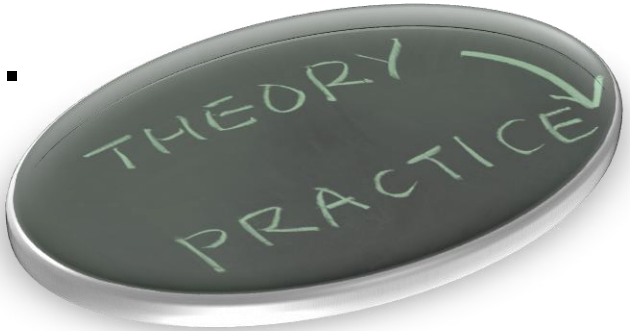
[DSZ15] D. Demmler, T. Schneider, M. Zohner.
ABY–a framework for efficient mixed-protocol secure two-party computation. In *NDSS 2015.*

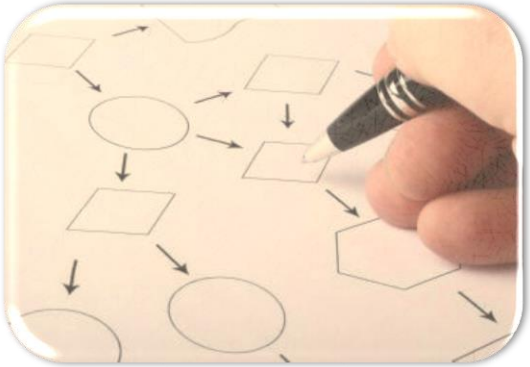
Experimental Results – UC Compiler

	UC Compiler		ABY Framework	
Private function (circuit size)	**UC Compile (ms)**	**UC I/O (ms)**	**PFE (GMW) (ms)**	**PFE (Yao) (ms)**
MULT32 **7 103**	329	1443	1092	540
DES **19 656**	1596	4174	2695	1311
AES **27 429**	2104	5064	5522	2349
MD5 **43 874**	4043	8785	7041	3548

Conclusion

Valiant's universal circuit is practical.





Embedding algorithm

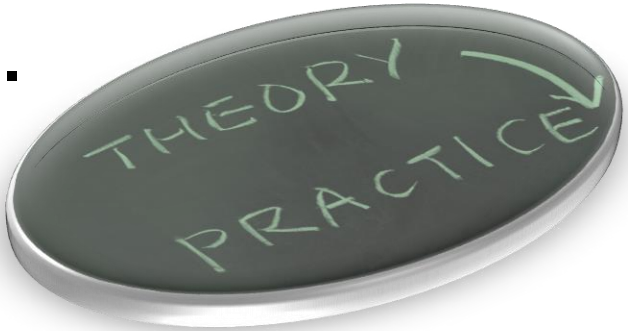
Refined size of construction

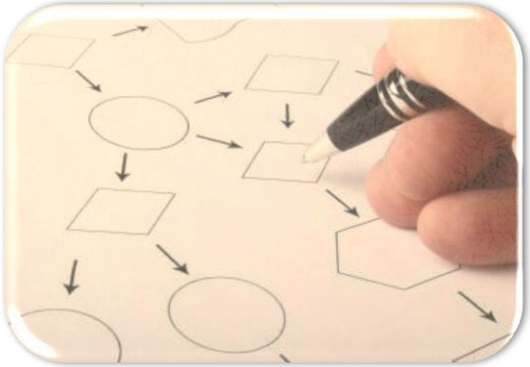
UC compiler

Conclusion

Valiant's universal circuit is practical.

Thank you for your attention!





Embedding algorithm

Refined size of construction

UC compiler

References

[Val76] L. G. Valiant: Universal circuits (preliminary report). In *STOC 1976.*

[KS08] V. Kolesnikov, T. Schneider: A practical universal circuit construction and secure evaluation of private functions. In *FC 2008*.

[MNPS04] D. Malkhi, N. Nisan, B. Pinkas, Y. Sella. Fairplay-Secure Two-Party Computation System. In *USENIX Security Symposium* 2004*.*

[MS13]: P. Mohassel, S. S. Sadeghian. How to hide circuits in MPC an efficient framework for private function evaluation. In *Eurocrypt 2013*.

[DSZ15] D. Demmler, T. Schneider, M. Zohner. ABY–a framework for efficient mixed-protocol secure two-party computation. In *NDSS 2015*.