Efficiently Protecting Data and Functions

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Thomas Schneider

CROSSING Summer School
September 13, 2019

Based on joint works with…

Ágnes
Kiss

Daniel
Demmler

Daniel
Günther

… and many more.

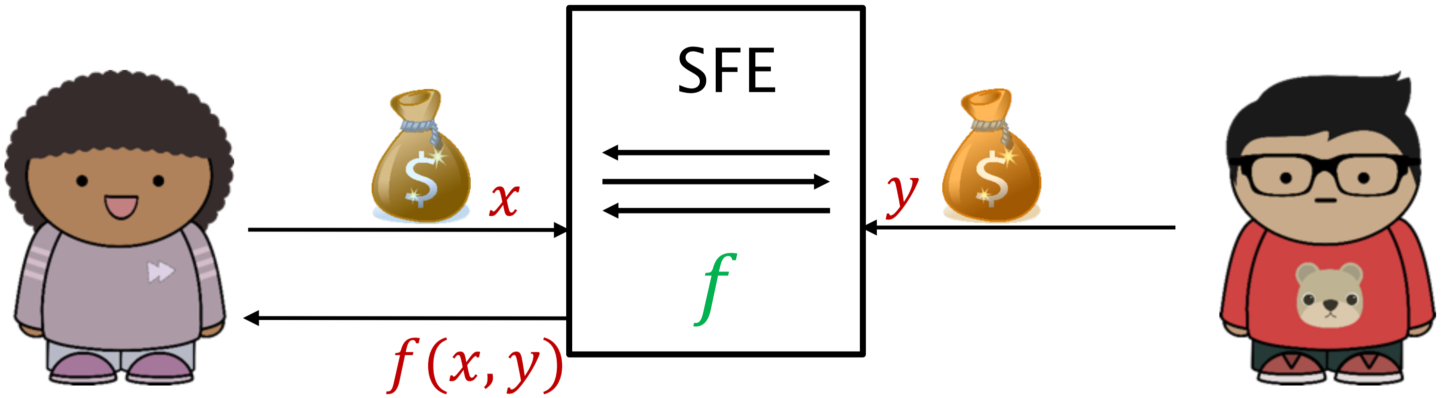
Outline

1. Secure Function Evaluation with Mixed Protocols
2. Private Function Evaluation of Boolean Circuits

Outline

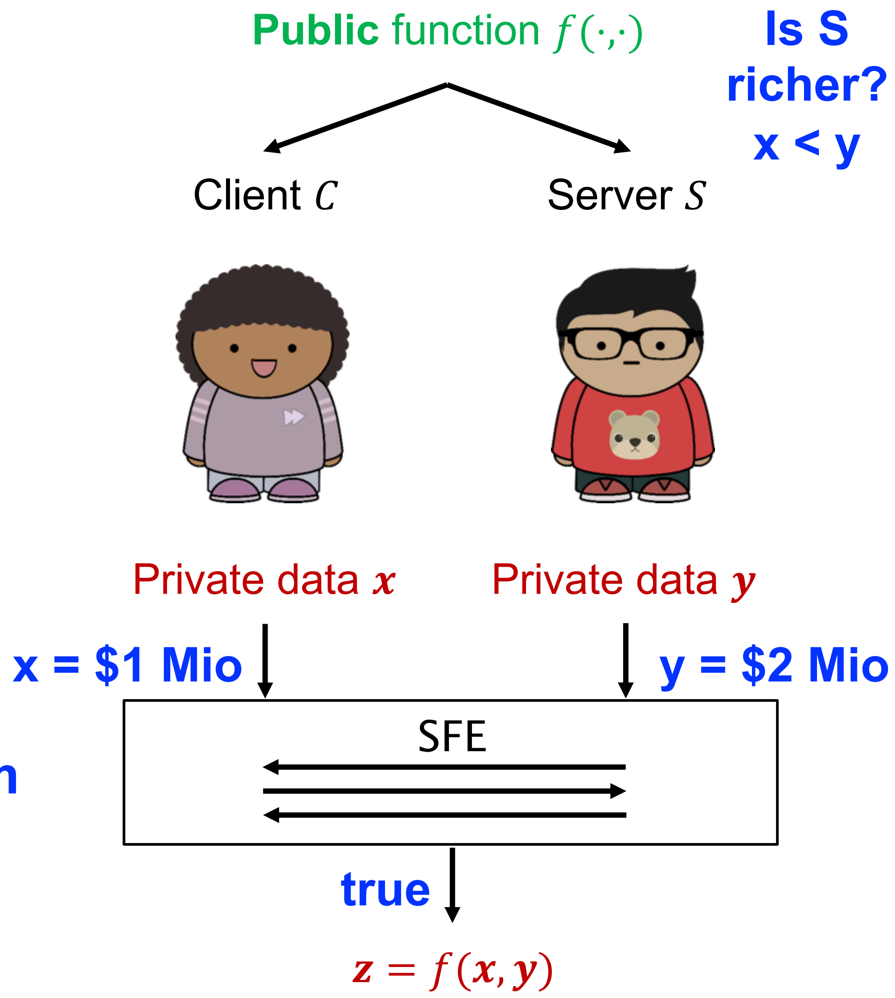
1. **Secure Function Evaluation with Mixed Protocols**
2. Private Function Evaluation of Boolean Circuits

Secure Function Evaluation (SFE)



Secure Function Evaluation (SFE)

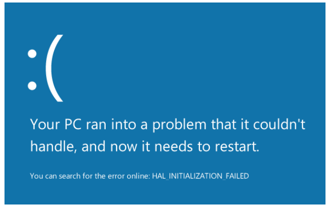
- compute arbitrary function f
- on private data $\boldsymbol{x}, \boldsymbol{y}$
- **without trusted third party**
- reveal nothing but result $\boldsymbol{z} = f(\boldsymbol{x}, \boldsymbol{y})$



Example: Yao's Millionaires' Problem

Applications of Secure Function Evaluation (Small Selection)

Auctions [NPS99], ...



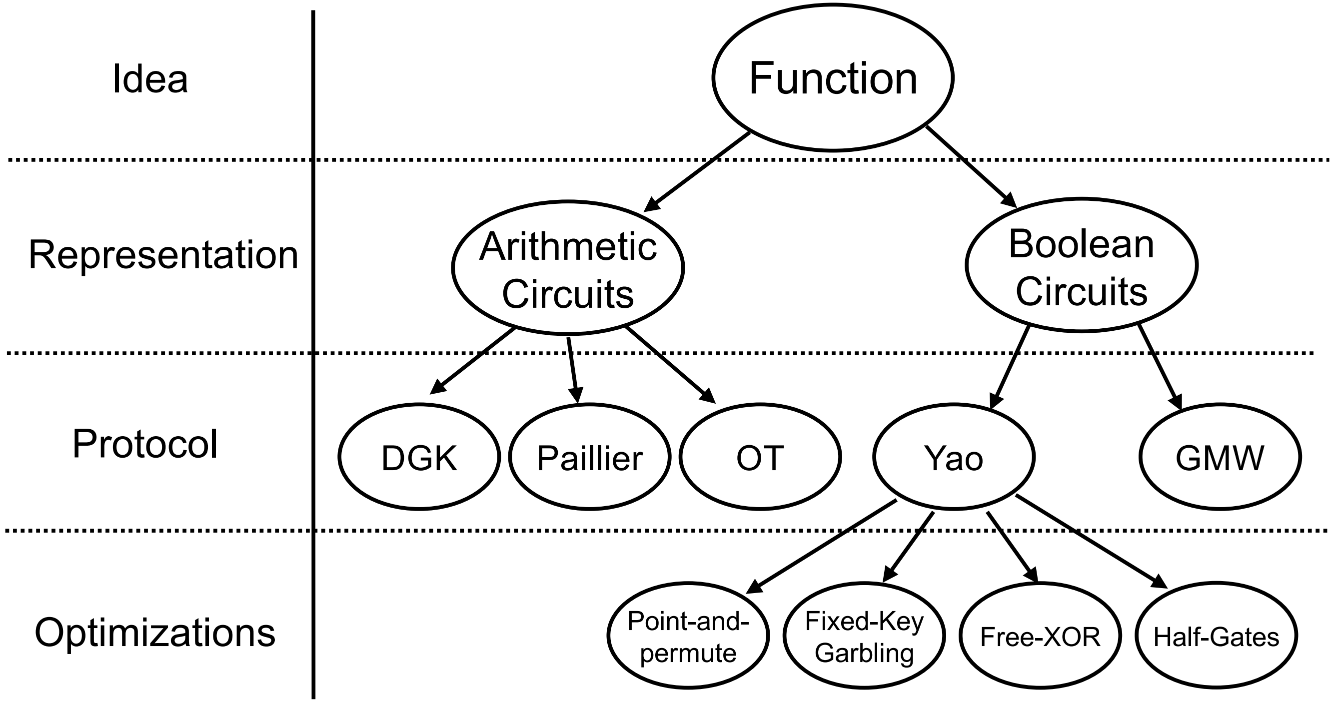
Remote Diagnostics [BPSW07], ...

DNA Searching [TKC07], ...

Biometric Identification [EFGKLT09], ...

Medical Diagnostics [BFKLSS09], ...

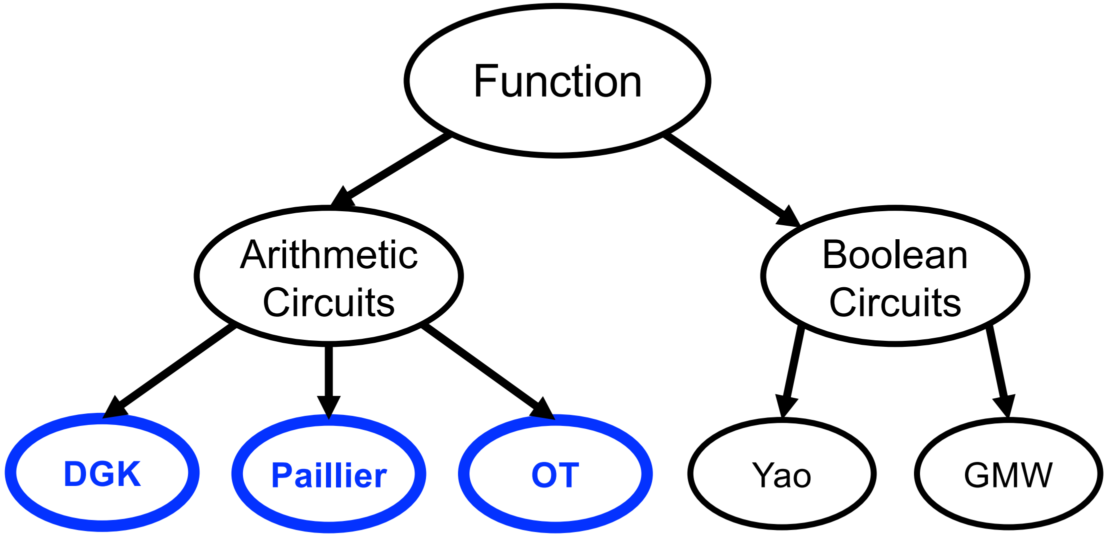
Implementing Secure Function Evaluation



Example for Mixed-Protocol SFE: Minimum Euclidean Distance

Minimum Euclidean Distance: $\min(\sum_{i=1}^{d}(\mathbf{S}_{i,1} - \mathbf{C}_i)^2, \ldots, \sum_{i=1}^{d}(\mathbf{S}_{i,n} - \mathbf{C}_i)^2)$

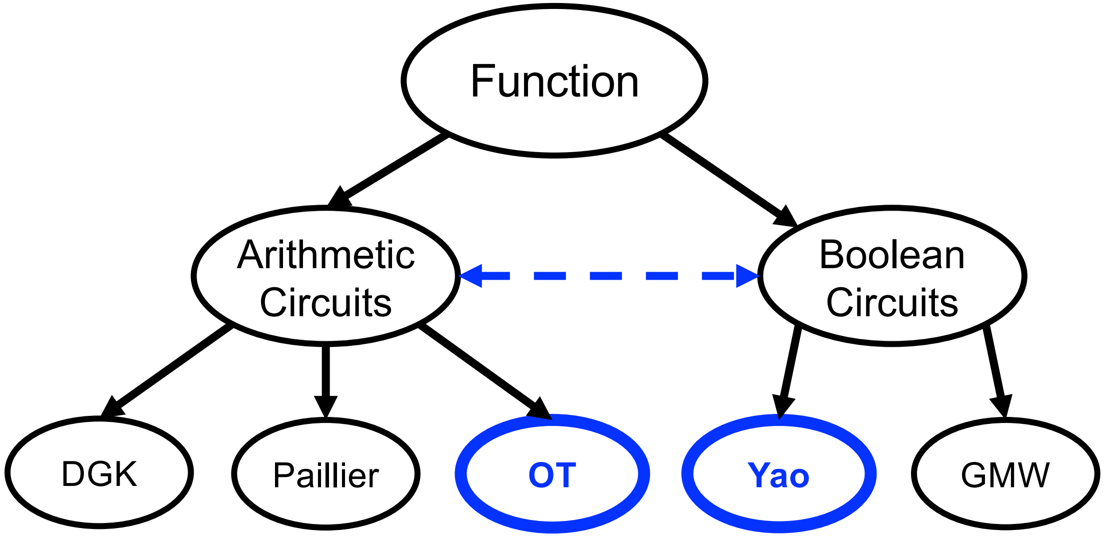
- Server holds database $\mathbf{S}$, client holds query $\mathbf{C}$
- Used in biometric matching (face-recognition, fingerprint, …)



Example for Mixed-Protocol SFE: Minimum Euclidean Distance

Minimum Euclidean Distance: $\min(\sum^{d}_{i=1}(\mathbf{S}_{i,1} - \mathbf{C}_i)^2, \ldots, \sum^{d}_{i=1}(\mathbf{S}_{i,n} - \mathbf{C}_i)^2)$

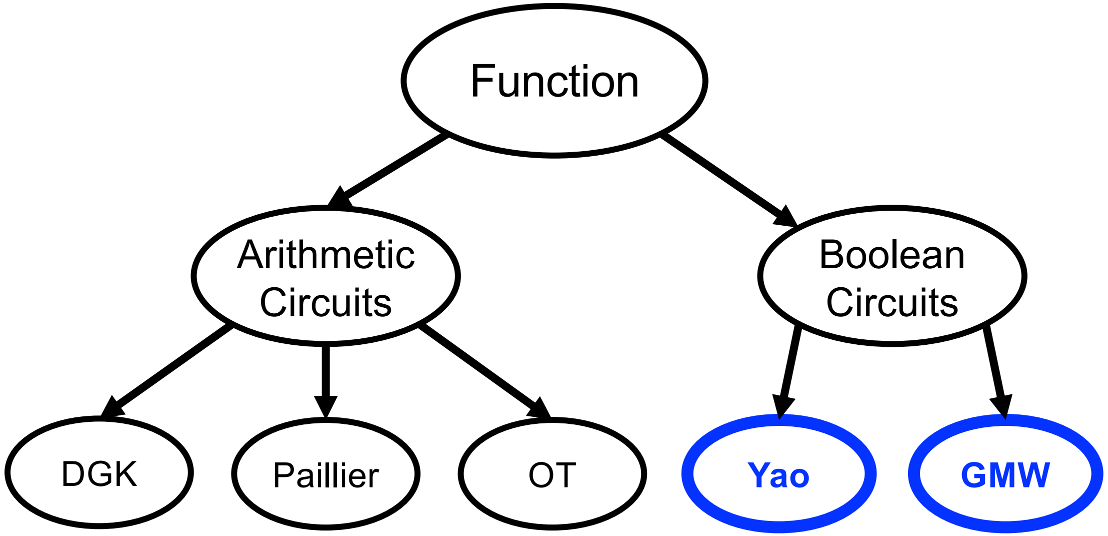
- Server holds database $\mathbf{S}$, client holds query $\mathbf{C}$
- Used in biometric matching (face-recognition, fingerprint, …)



Example for Mixed-Protocol SFE: Minimum Euclidean Distance

Minimum Euclidean Distance: $\min(\sum_{i=1}^{d}(\mathbf{S}_{i,1} - \mathbf{C}_i)^2, \ldots, \sum_{i=1}^{d}(\mathbf{S}_{i,n} - \mathbf{C}_i)^2)$

- Server holds database $\mathbf{S}$, client holds query $\mathbf{C}$
- Used in biometric matching (face-recognition, fingerprint, …)



The ABY Framework [DSZ15]

Arithmetic sharing: v = a + b mod 2^ℓ

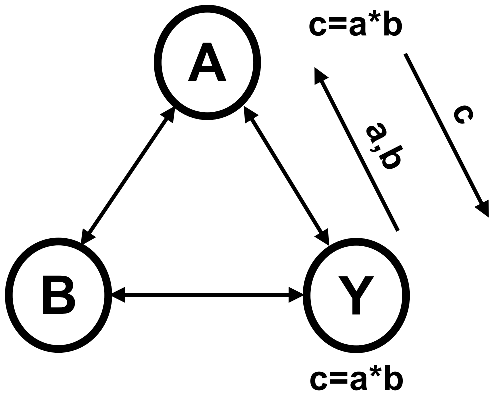
- Free addition / cheap multiplication
- Good for multiplication

Boolean sharing: v = a $\oplus$ b [GMW87]

- Free XOR / one message per AND
- Good for multiplexing

Yao's garbled circuits: S: k_0,k_1; C: k_v [Yao86]

- Free XOR / no interaction per AND
- Good for comparison



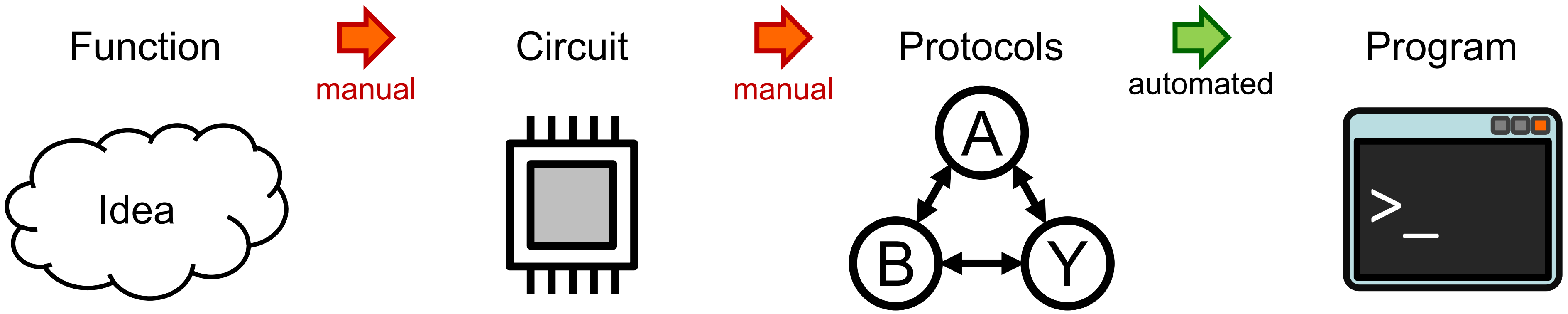
Multiplication (32-bit)		
Protocol	***Yao***	***Mixed***
LAN [µs]	**1.1**	**0.1**
Comm. [KB]	**100**	**5**

[D**S**Z15] D. Demmler, T. Schneider, M. Zohner: ABY – A Framework for Efficient Mixed-Protocol Secure Two-party Computation. In *NDSS'15.*

The ABY Framework [DSZ15]

C++-Framework for efficient hybrid SFE

- Efficient secure two-party computation protocols & conversions using symmetric crypto
- Code: https://encrypto.de/code/ABY

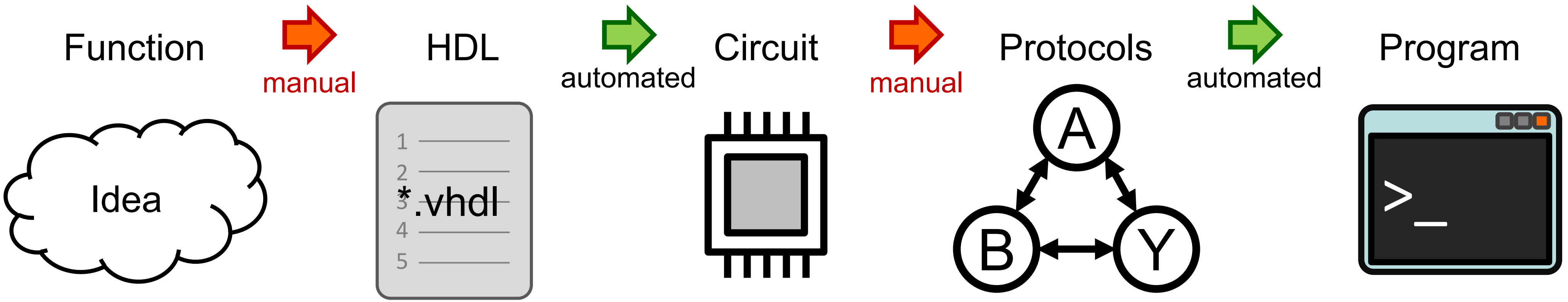


[DSZ15] D. Demmler, T. Schneider, M. Zohner: ABY – A Framework for Efficient Mixed-Protocol Secure Two-party Computation. In *NDSS'15.*

HDL Circuits [DDKSSZ15]

Compilation from HDL into SFE and efficient building blocks

- Function description in Verilog/VHDL (or via high-level synthesis in C)
- Extends TinyGarble by hardware synthesis for depth-optimized circuits:
  [SHS**S**K15] E. Songhori, S. Hussain, A.-R. Sadeghi, T. Schneider, F. Koushanfar:
  TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits. In *S&P'15.*

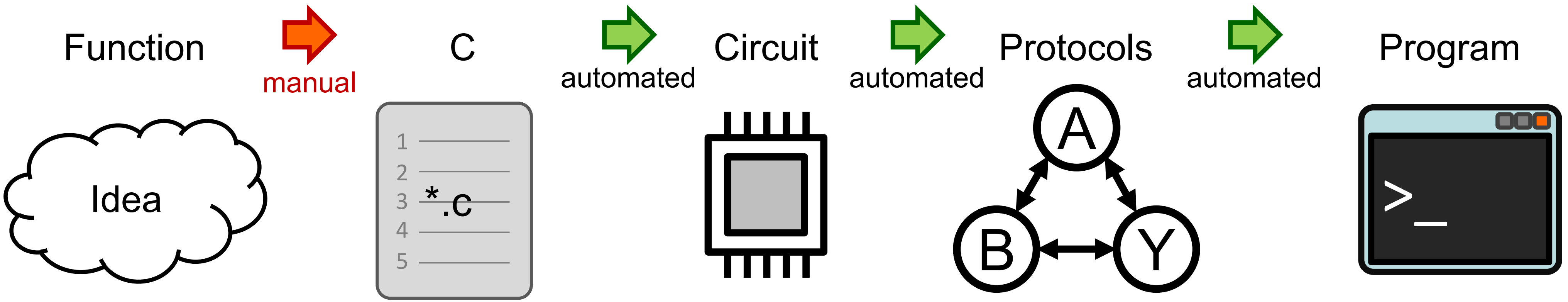


[DDKS**S**Z15] D. Demmler, G. Dessouky, F. Koushanfar, A.-R. Sadeghi, T. Schneider, S. Zeitouni. Automated Synthesis of Optimized Circuits for Secure Computation. In *CCS'15.*

HyCC [BDKK<u>S</u>18]

Fully automated compilation from C into hybrid SFE

- Extension of CBMC-GC and combination with ABY: [HFKV12] A. Holzer, M. Franz, S. Katzenbeisser, H. Veith: Secure Two-party Computations in ANSI C. In *CCS'12*.
- Automated partitioning and protocol selection



[BDKK**S**18] N. Büscher, D. Demmler, S. Katzenbeisser, D. Kretzmer, T. Schneider. HyCC: Compilation of Hybrid Protocols for Practical Secure Computation. In *CCS'18.*

HyCC – Hybrid MPC Applications

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Protocol online runtime: Biometric Matching (n=1000)

	Runtime LAN	Runtime WAN
Yao GC (Y)	1,177 ms	1,789 ms
GMW (B)	2,932 ms	7,974 ms
LSS and GMW (A+B)	131 ms	4,249 ms
LSS and Yao GC (A+Y)	**70 ms**	**584 ms**

Protocol online runtime: Textbook Gauss Solver (n=10)

	Runtime LAN	Runtime WAN	Total Communication
Y	429 ms	**631 ms**	31 MB
A + Y	**256 ms**	4,235 ms	**10 MB**

Protocol online runtime: MiniONN CNN (Relu, MNIST dataset)

	Runtime LAN	Runtime WAN
[LJLA17]	5,740 ms	-
A + Y	**1,621 ms**	5,882 ms

All circuits compiled with HyCC and evaluated in the ABY framework.

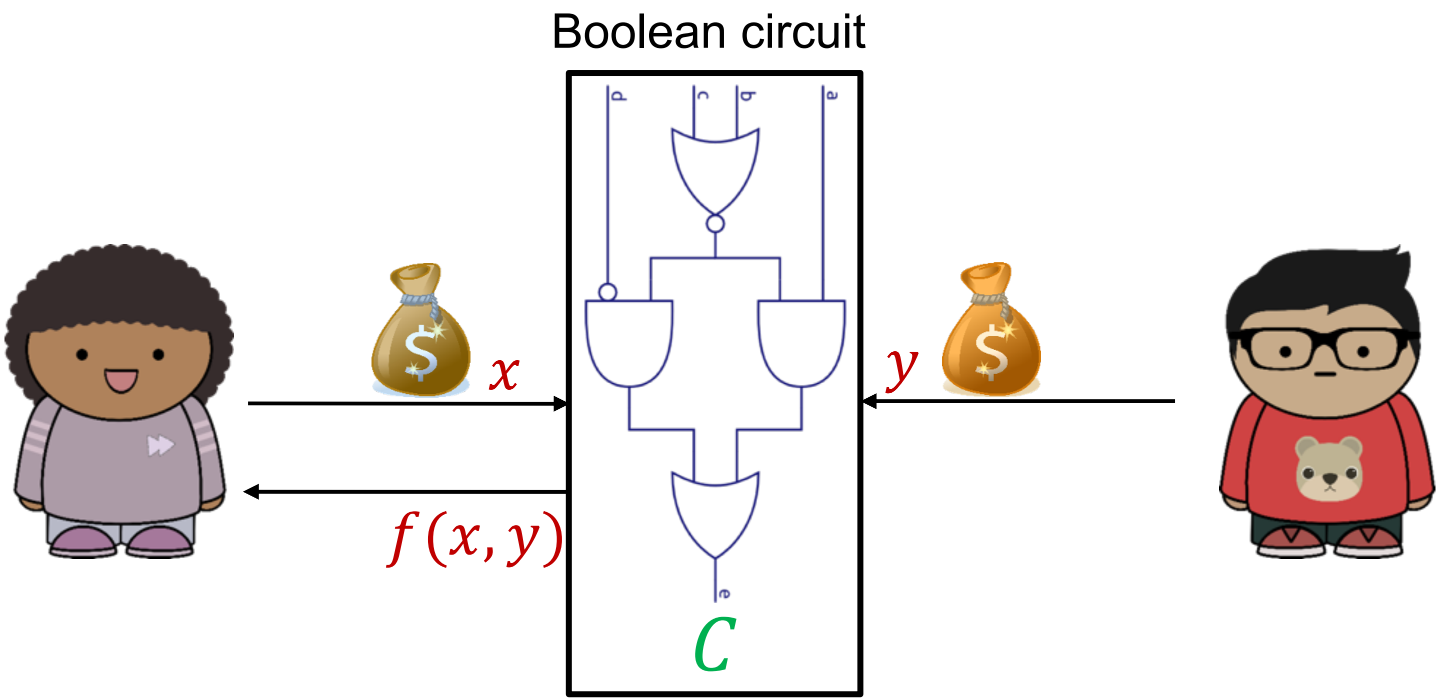
LAN: 1Gbit / WAN: 100Mbit and 100ms RTT.

Outline

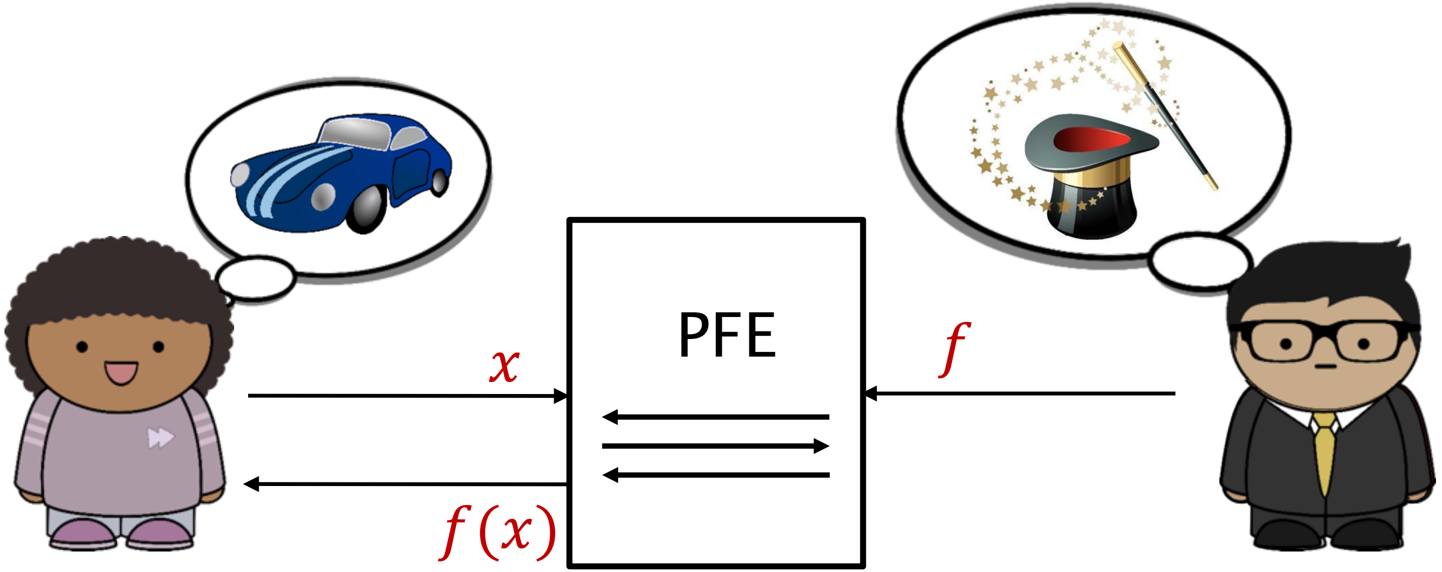
1. Secure Function Evaluation with Mixed Protocols

2. Private Function Evaluation of Boolean Circuits

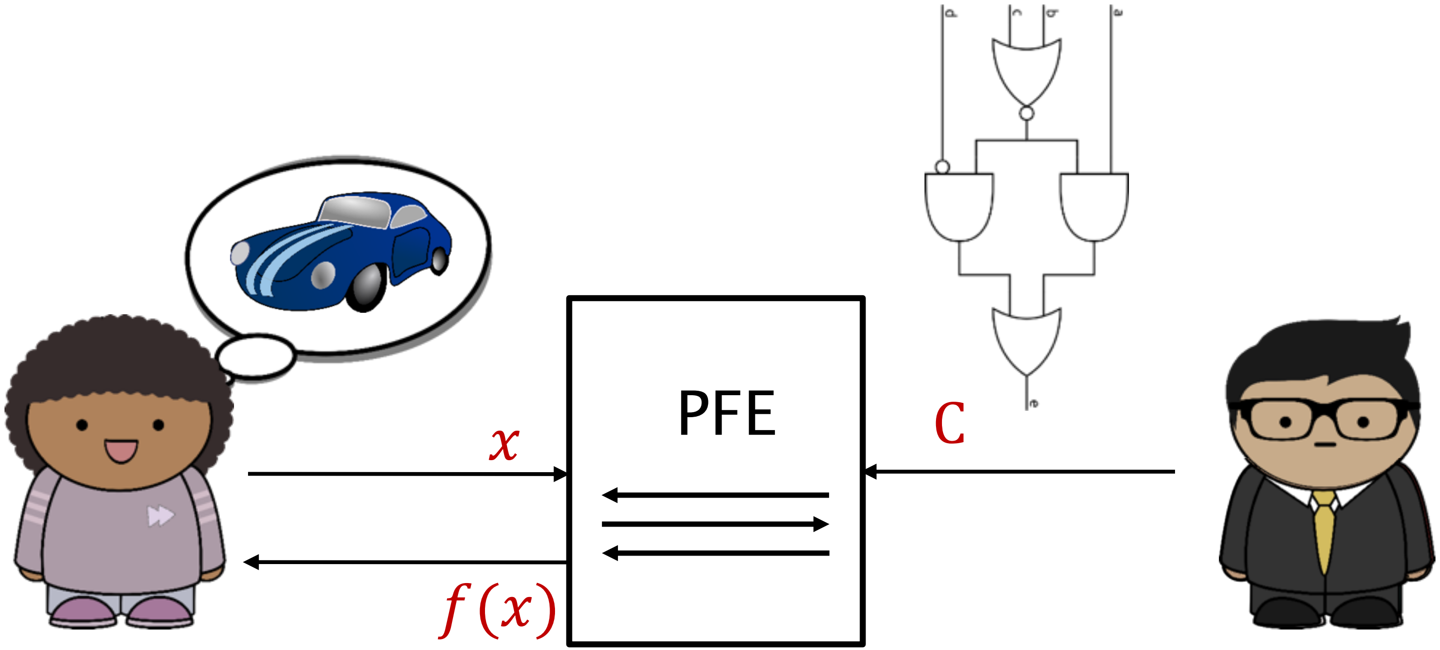
Secure Function Evaluation of Boolean Circuits



Private Function Evaluation (PFE)



Private Function Evaluation of Boolean Circuits



Applications of PFE of Boolean Circuits

Solvency verification

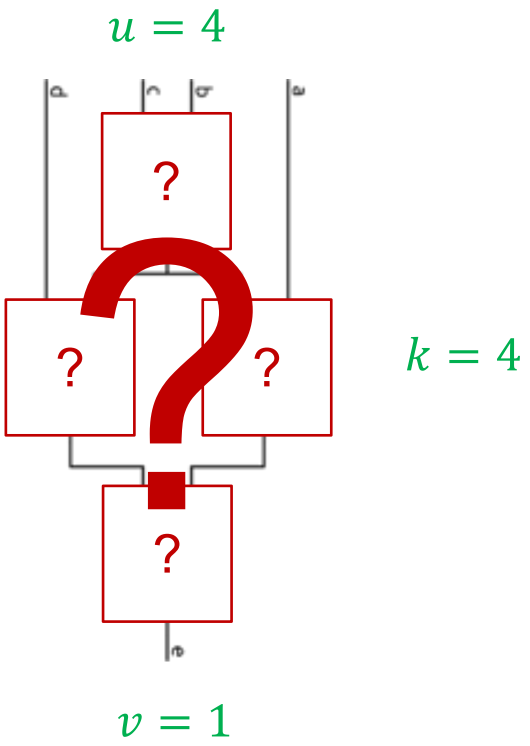
Smart metering

Private databases

Insurance rate & credit risk assessment

Challenges – Hiding the Circuit

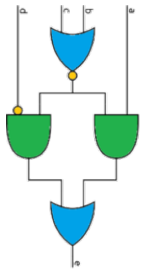
- Public:
  - Number of inputs u
  - Number of outputs v
  - Number of gates k
- Private:
  - Functionality of gates
  - Topology of circuit



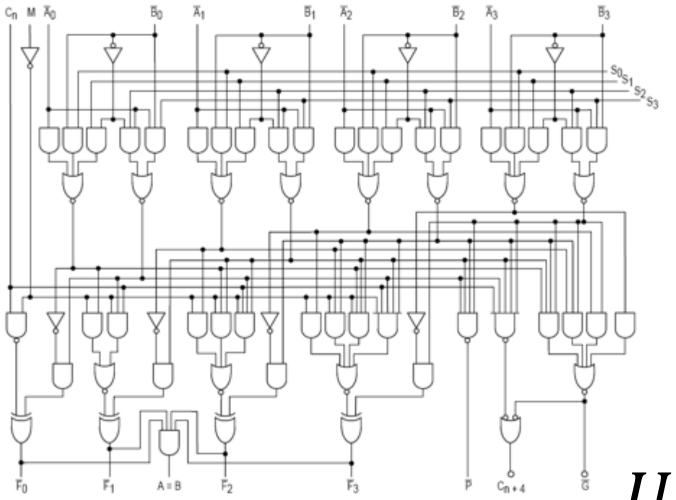
Universal Circuit (UC)

There exists a Boolean circuit UC of size $\Theta(n \log n)$ s.t.
for any Boolean function f of size n
UC can be programmed to compute f.

Leslie G. Valiant
1976



f



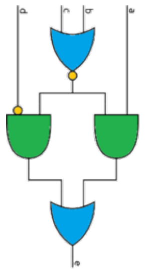
UC

Universal Circuit (UC)

There exists a Boolean circuit UC of size $\Theta(n \log n)$ s.t.
for any Boolean function f of size n
there exists a programming p
such that for any input x: $UC(p, x) = f(x)$.

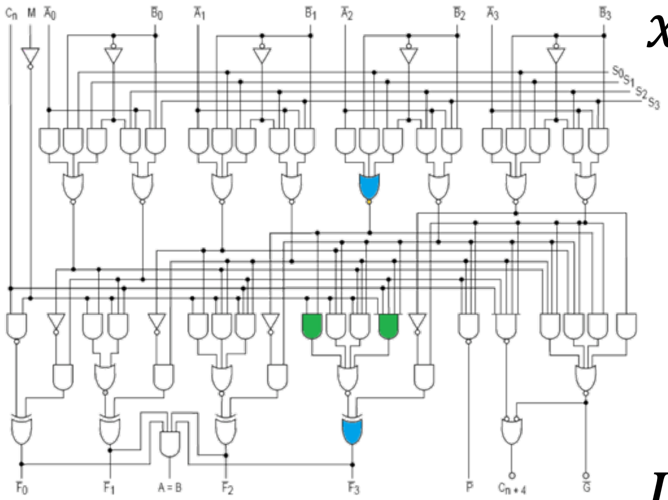
Leslie G. Valiant
1976

x



$f(x)$

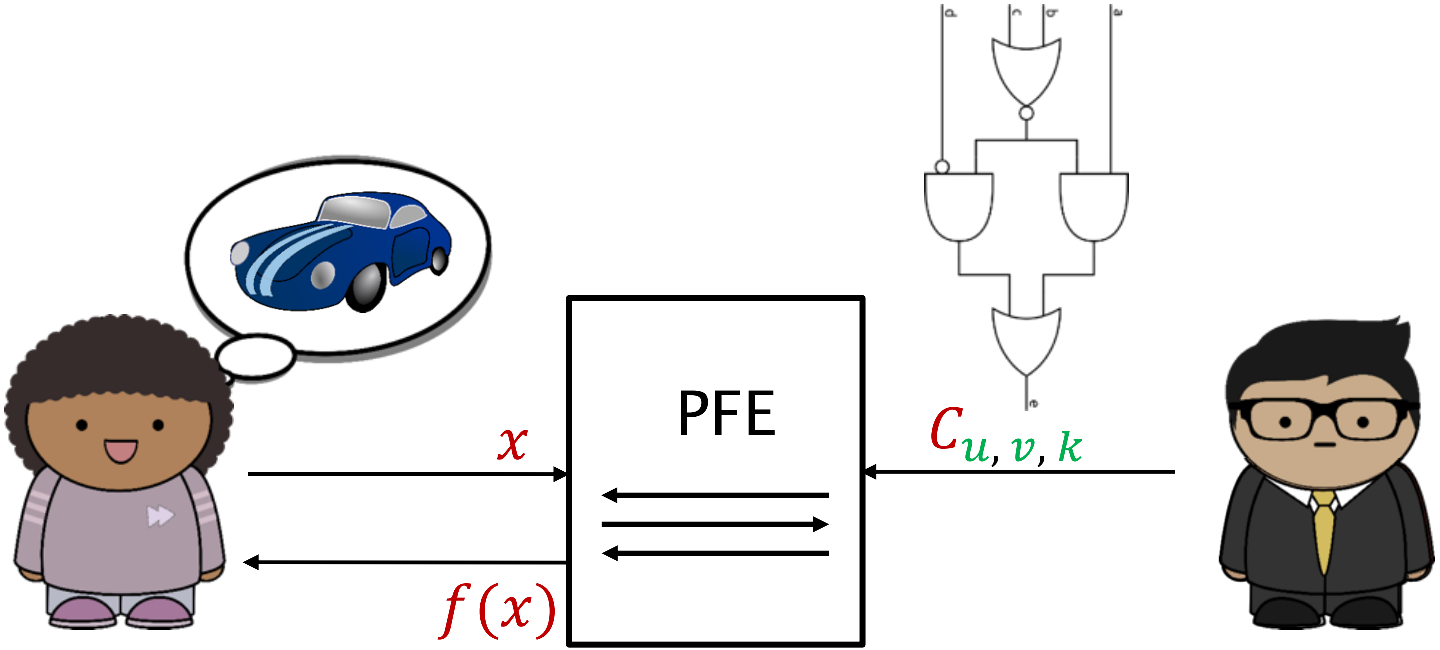
p →



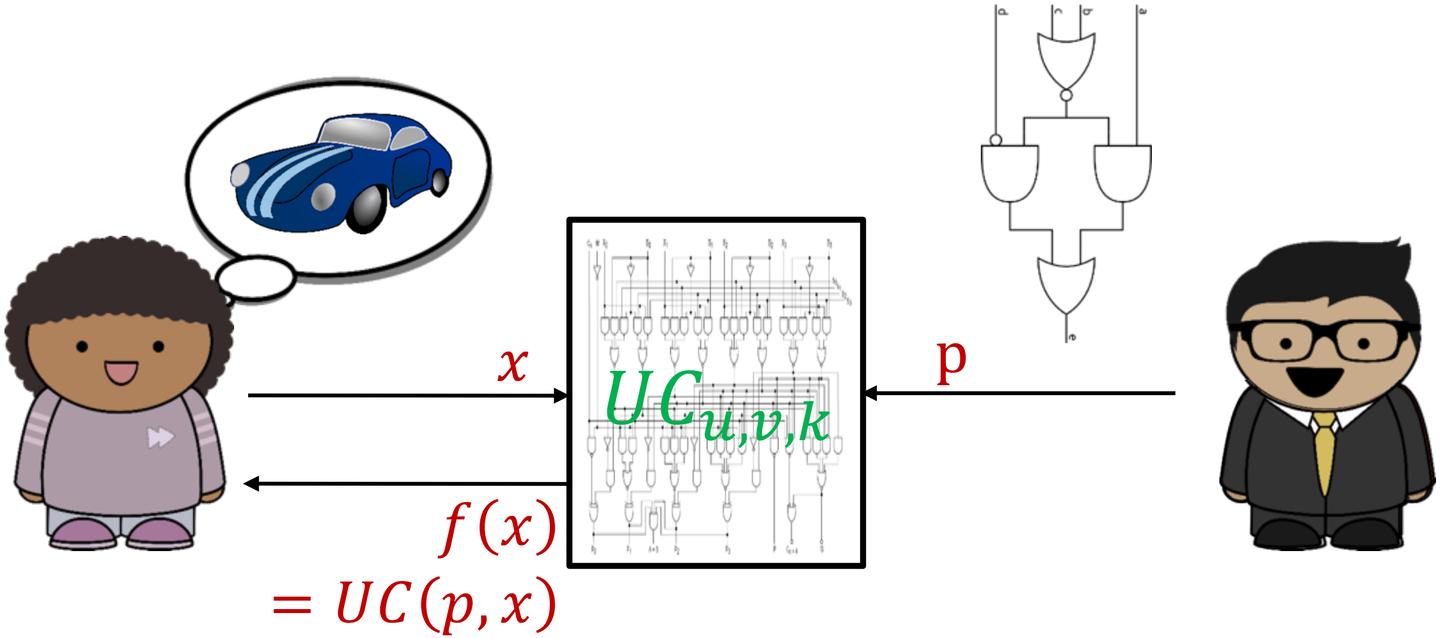
x

$UC(p, x) = f(x)$

PFE of Boolean Circuits



PFE of Boolean Circuits via SFE of a UC



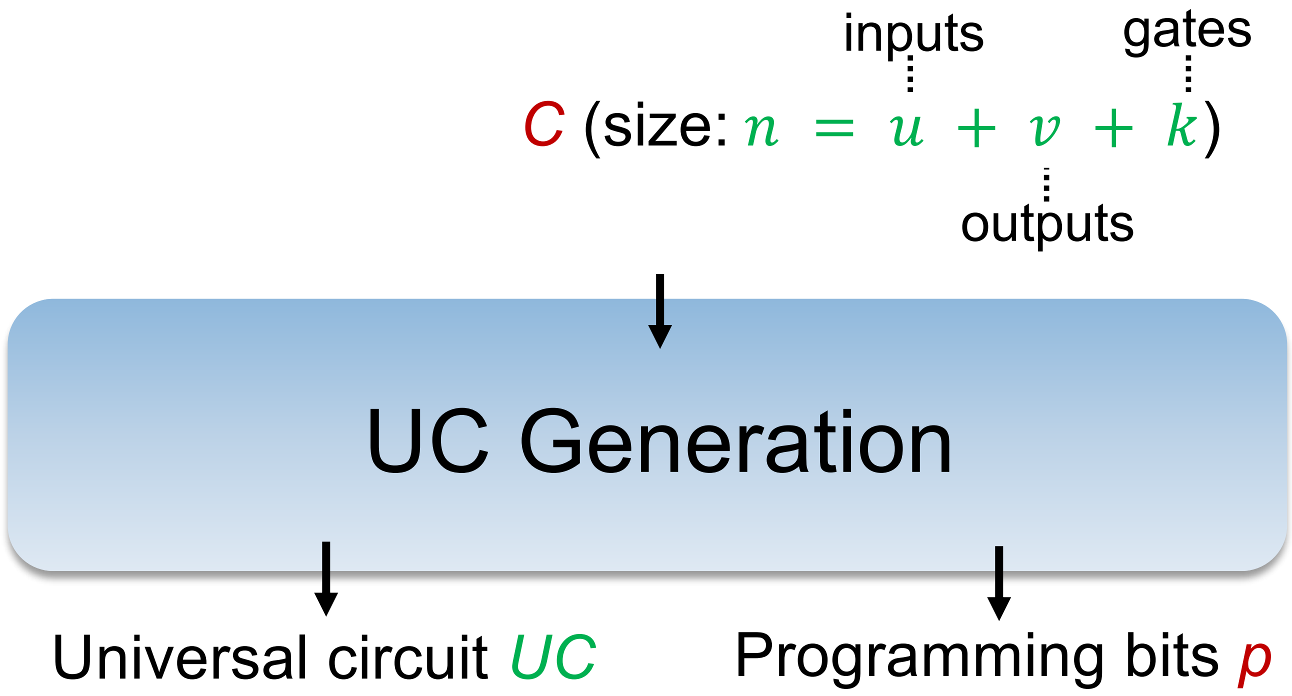
Further Applications of UCs beyond PFE

Obfuscation

Attribute-based Encryption

Batch Execution MPC

Adaptively Secure MPC


inputs
gates
C (size: $n = u + v + k$)
outputs
UC Generation
Universal circuit UC
Programming bits p

Existing UC Constructions

	[Val76] 2-way	[Val76] 4-way
Size	$5n \log n$	$4.75n \log n$
Depth	$3n$	$3.75n$
Code	✗	✗

[Val76] L. G. Valiant: Universal Circuits (Preliminary Report). In *STOC'76.*

Valiant's UC Construction

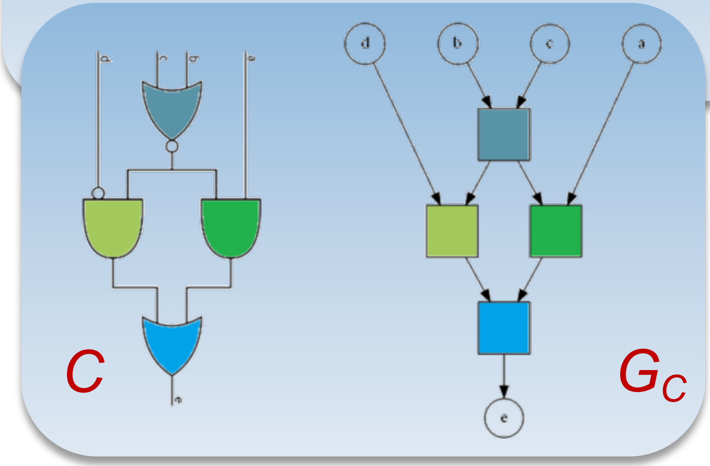
ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

n

C size $\leq n$

↓

Graph G_C



Valiant's UC Construction

GENERATION

n

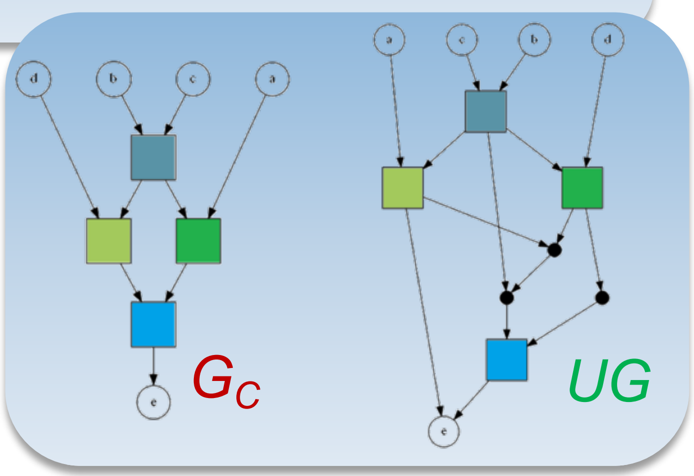
C size $\leq n$

Graph G_C

Universal graph UG → Embedding E

Universal circuit UC

PROGRAMMING



Valiant's UC Construction

GENERATION

n

Universal graph UG → Embedding E

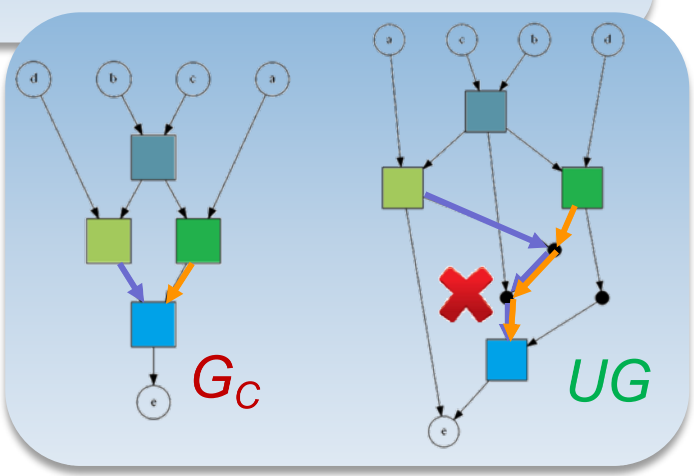
Universal circuit UC

C size $\leq n$

Graph G_C

Embedding E

PROGRAMMING



Valiant's UC Construction

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

n

C size $\leq n$

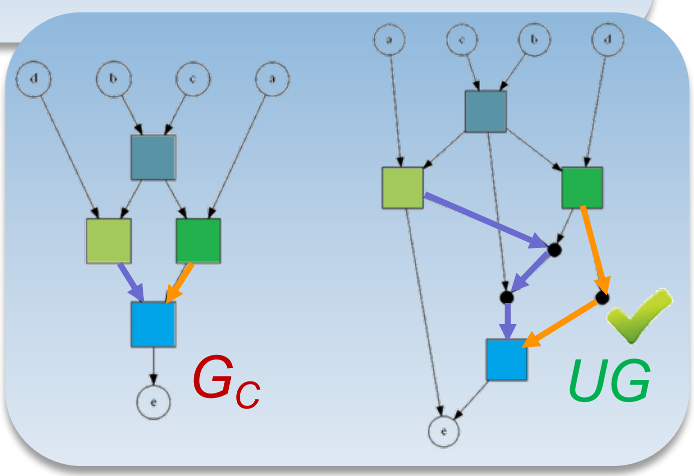
GENERATION

Graph G_C

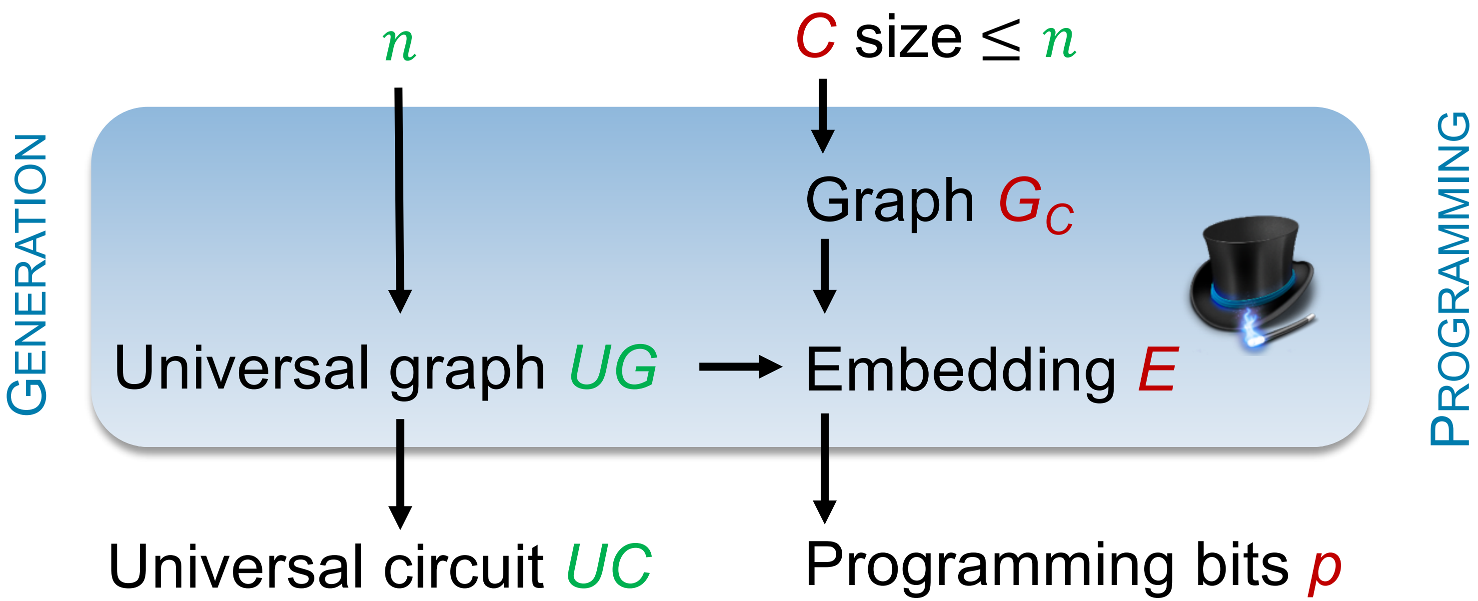
Universal graph UG → Embedding E

Universal circuit UC

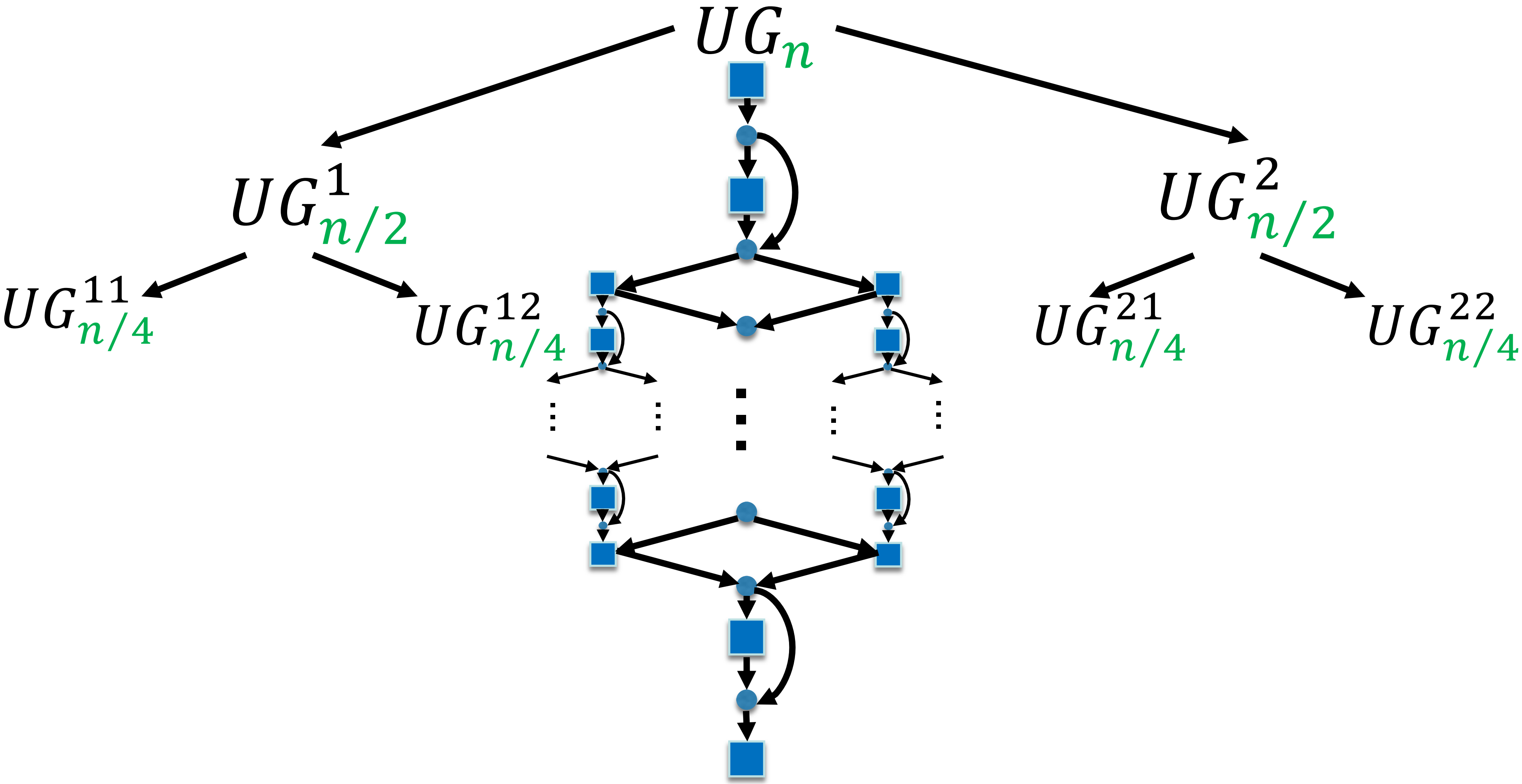
PROGRAMMING



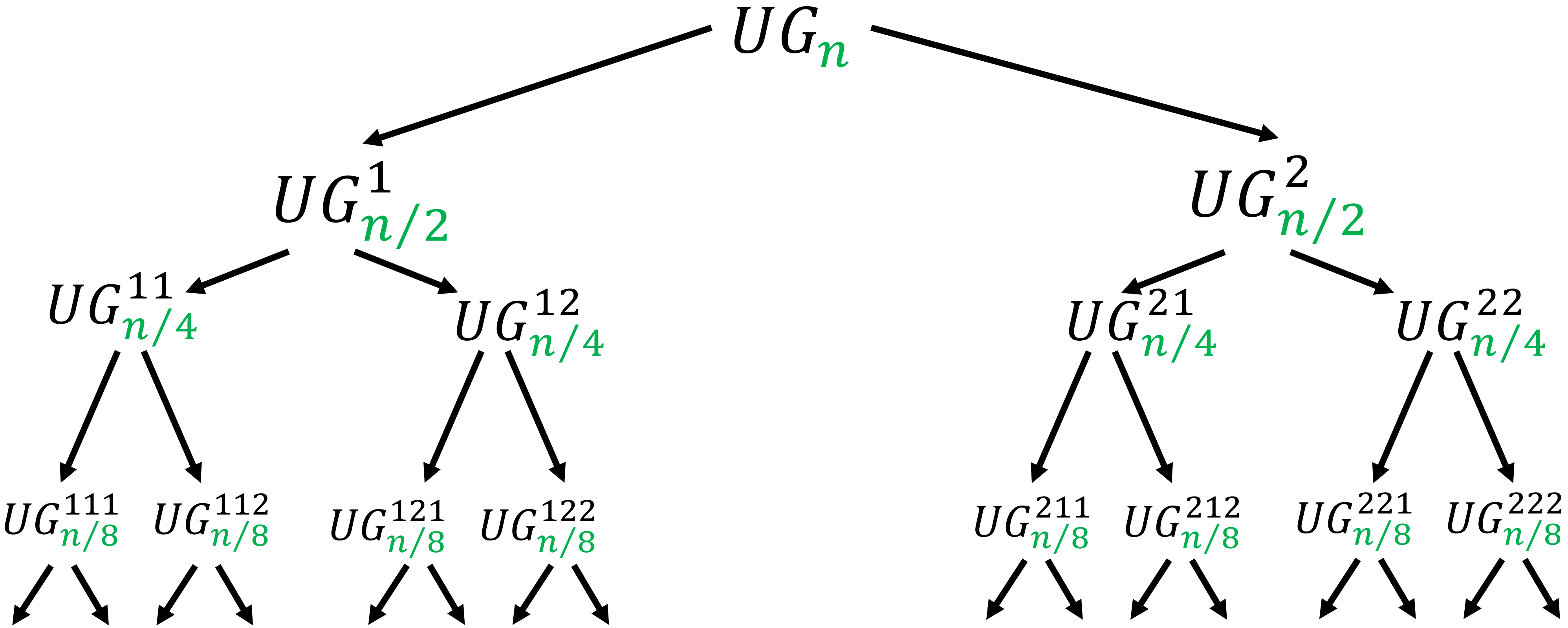
Valiant's UC Construction



2-way Recursive UG Construction



2-way Recursive UG Construction



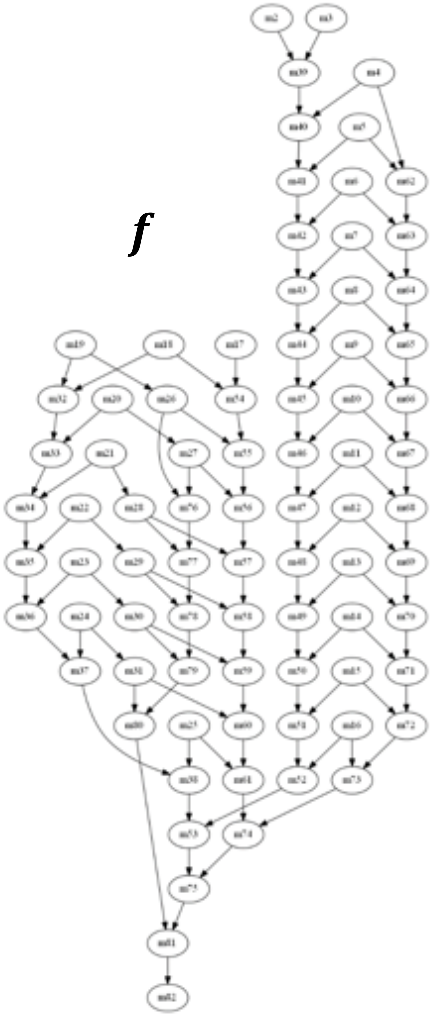
A „Small„ Example

$u = 25$

$k = 56$

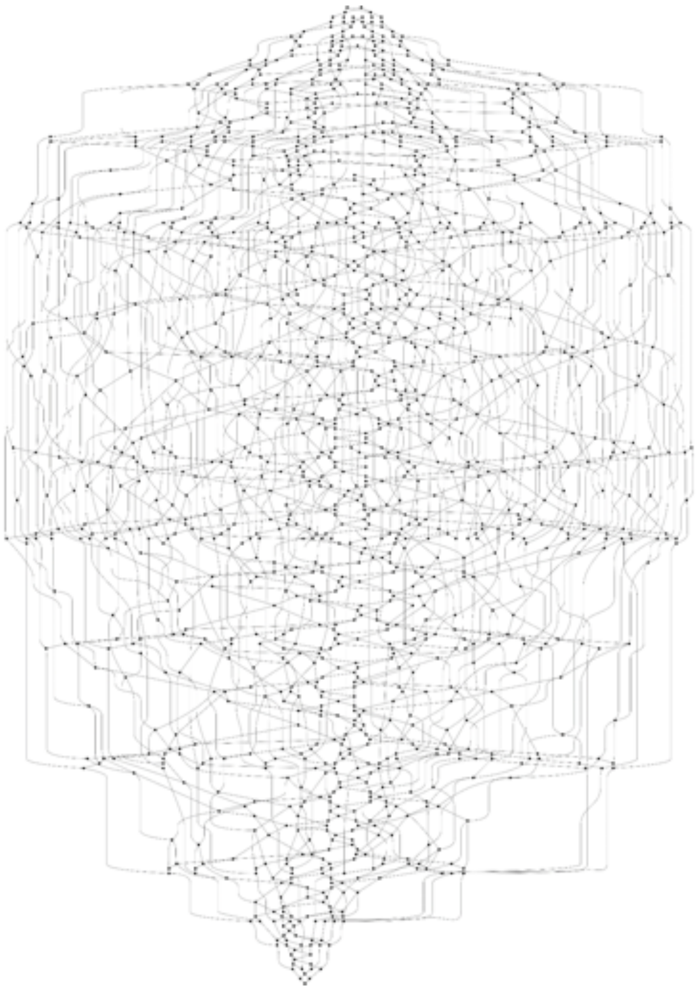
$v = 1$

$\boldsymbol{f}$



$\boldsymbol{UC}$

835 nodes /
869 AND gates



Existing UC Constructions

	[Val76] 2-way	[Val76] 4-way	[KS08]
Size	$5n \log n$	$4.75n \log n$	$1.5n \log^2 n + 2n \log n$
Depth	$3n$	$3.75n$	$n \log n$
Code	✗	✗	✓

[KS08] V. Kolesnikov, T. Schneider: A Practical Universal Circuit Construction and Secure Evaluation of Private Functions. In *FC'08*.

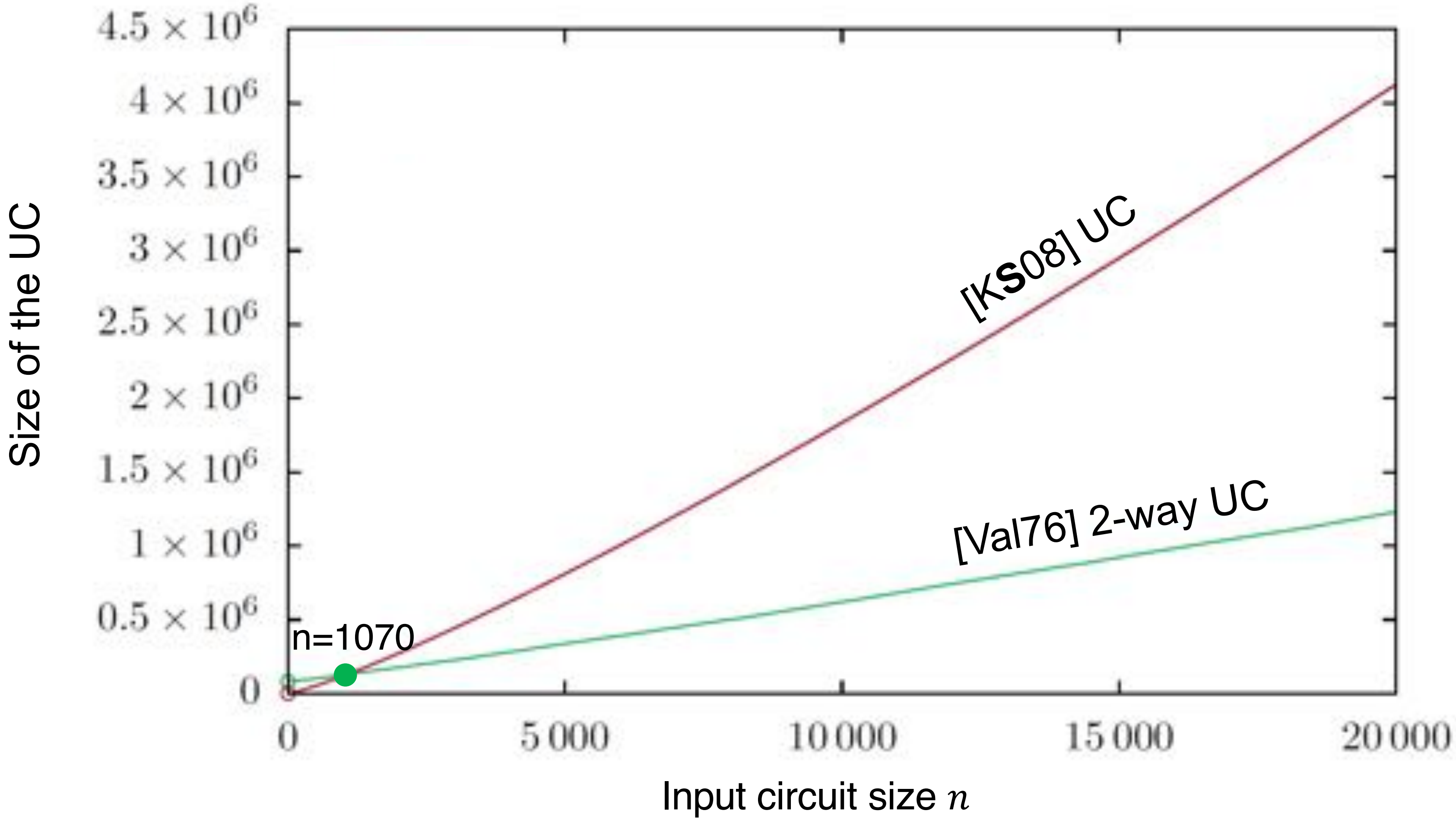
Existing UC Constructions

	[Val76] 2-way	[Val76] 4-way	[KS08]
Size	$5n \log n$	$4.75n \log n$	$1.5n \log^2 n + 2n \log n$
Depth	$3n$	$3.75n$	$n \log n$
Code	✓	✗	✓

[KS16] Á. Kiss, T. Schneider: Valiant's Universal Circuit is Practical. In *EUROCRYPT'16.*

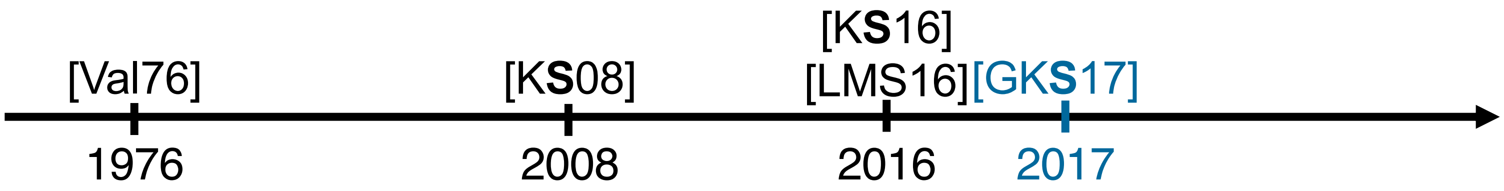
[LMS16] H. Lipmaa, P. Mohassel, S. Sadeghian: Valiant's Universal Circuit: Improvements, Implementation, and Applications. In *ePrint 2016/017.*

Comparison



Size of the UC
4.5×10^6
4×10^6
3.5×10^6
3×10^6
2.5×10^6
2×10^6
1.5×10^6
1×10^6
0.5×10^6
0
0
5 000
10 000
15 000
20 000
Input circuit size n
[KS08] UC
[Val76] 2-way UC
n=1070

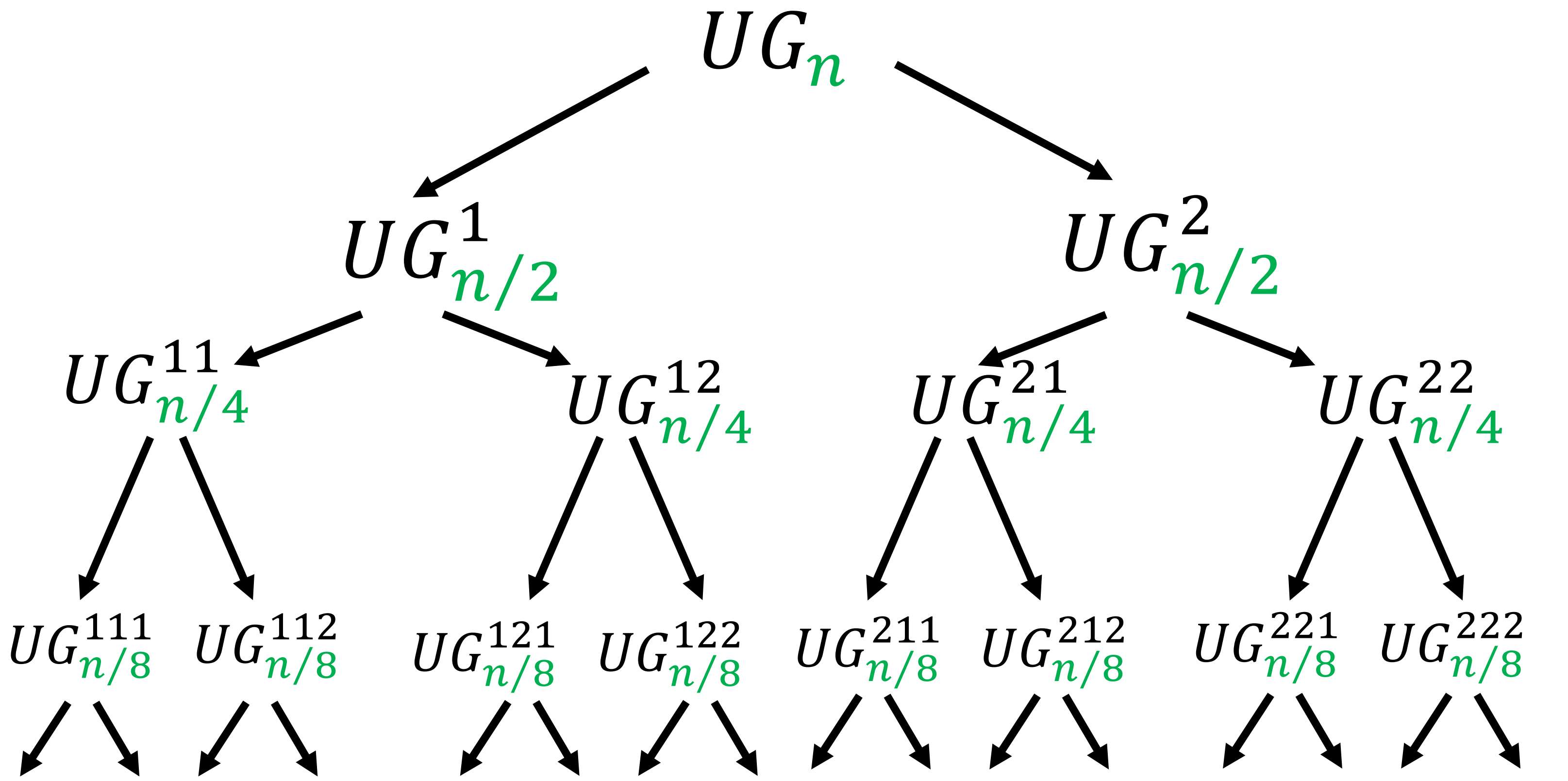
Existing UC Constructions



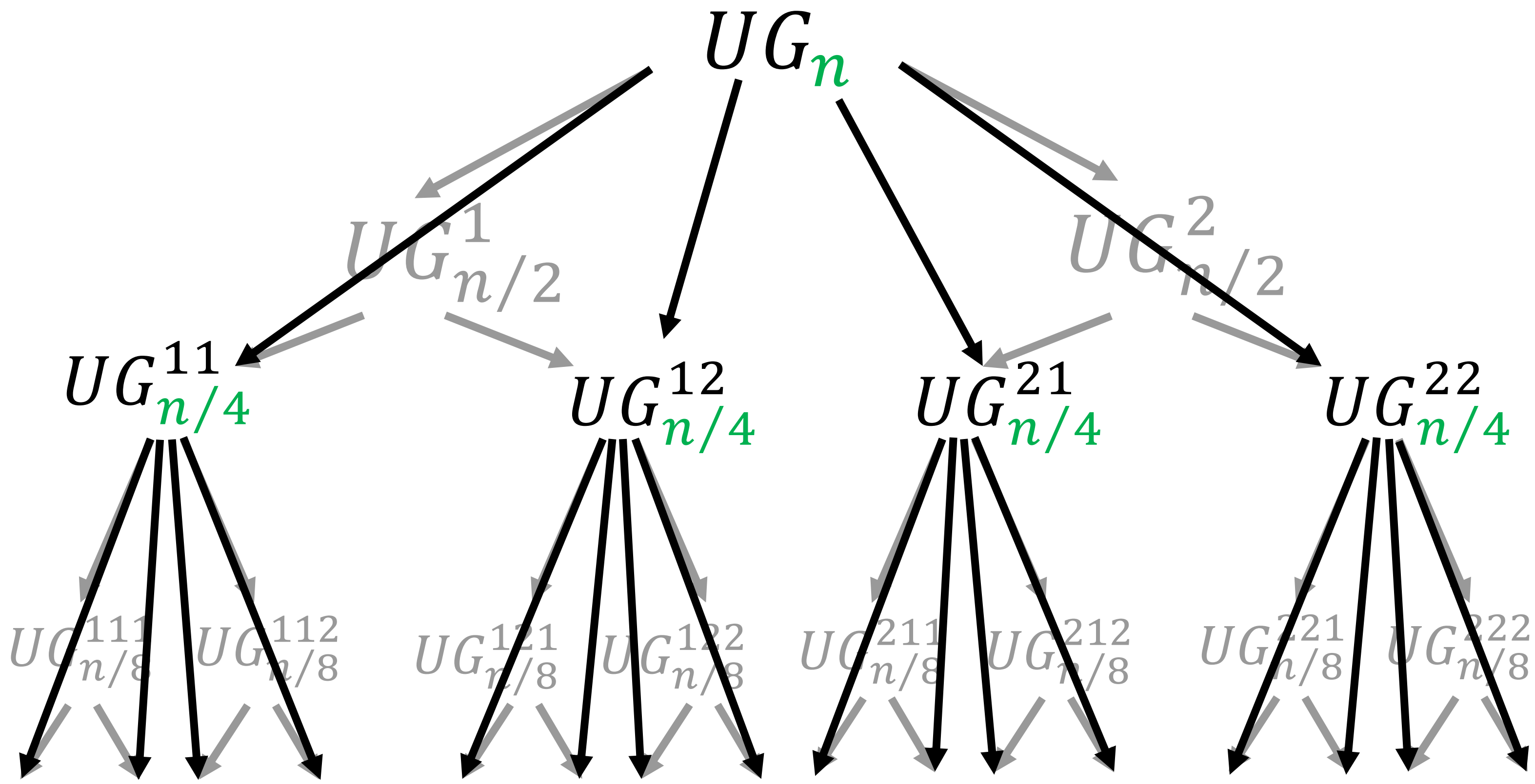
	[Val76] 2-way	[Val76] 4-way	[KS08]
Size	$5n\log n$	$4.75n\log n$	$1.5n\log^2 n + 2n\log n$
Depth	$3n$	$3.75n$	$n\log n$
Code	✓	✓	✓

[GK**S**17] D. Günther, Á. Kiss, T. Schneider: More Efficient Universal Circuit Constructions. In *ASIACRYPT'17.*

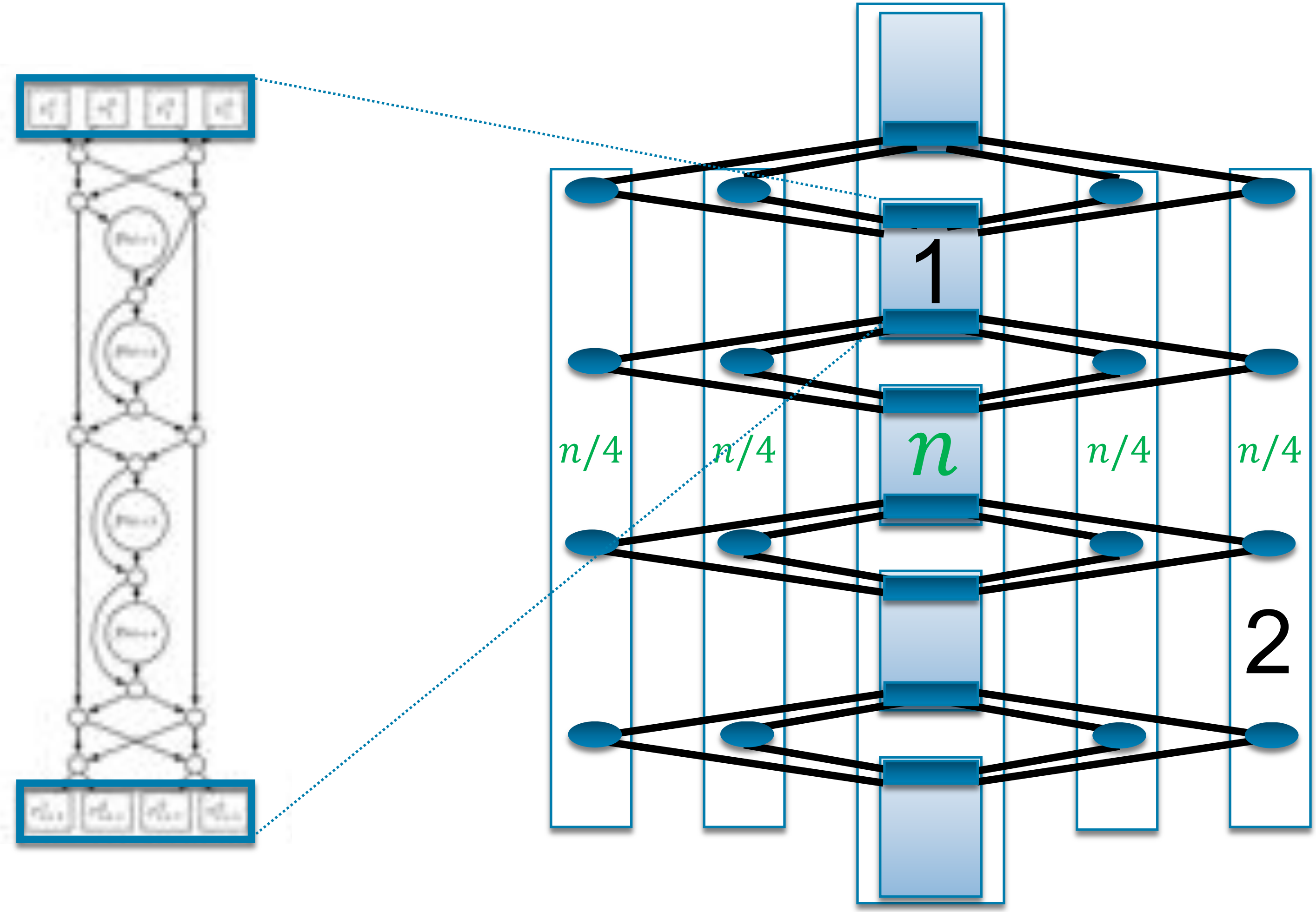
2-way Recursive UG Construction [Val76]



4-way Recursive UG Construction [Val76]



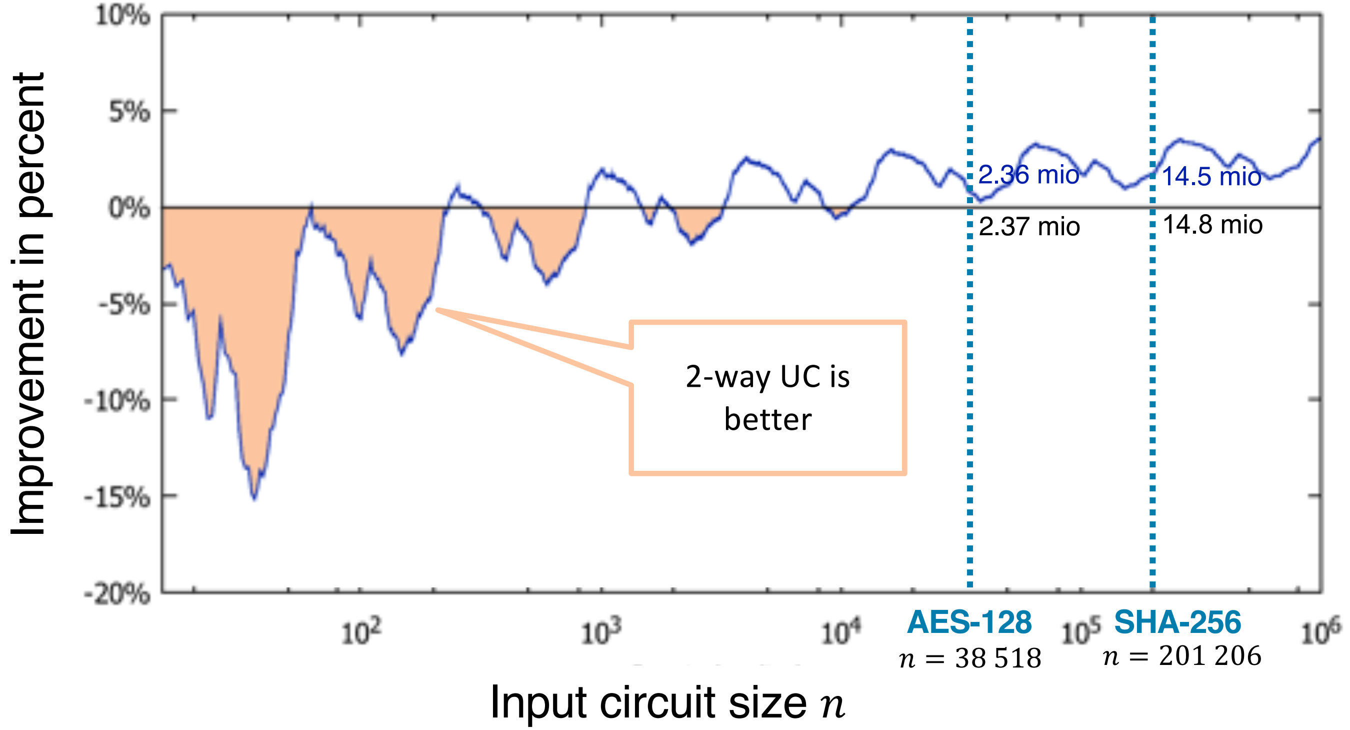
4-way Modular Embedding Algorithm



Task 1:
Block embedding

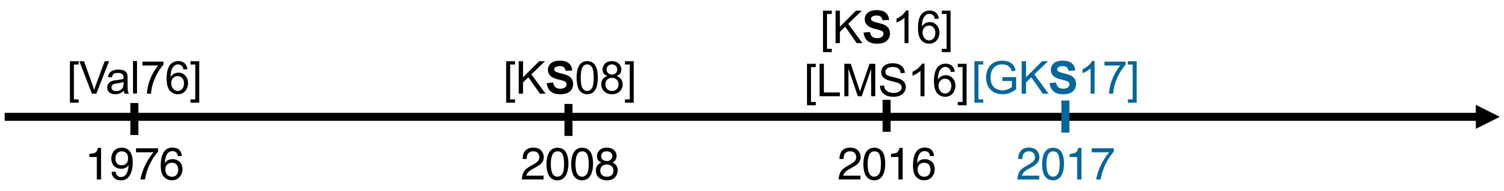
Task 2:
Recursion point embedding

Blue: Improvement of 4-way UC over 2-way UC



Maximum: $\frac{5}{4.75} - 100\% = 5.3\%$

Existing UC Constructions



	[Val76] 2-way	[Val76] 4-way	[KS08]	[GKS17] Hybrid(2,4)
Size	$5n \log n$	$4.75n \log n$	$1.5n \log^2 n$ $+ 2n \log n$	$4.75n \log n$
Depth	$3n$	$3.75n$	$n \log n$	$3.75n$
Code	✓	✓	✓	✗

[GKS17] D. Günther, Á. Kiss, T. Schneider: More Efficient Universal Circuit Constructions. In *ASIACRYPT'17.*

Hybrid UC

UC for size n

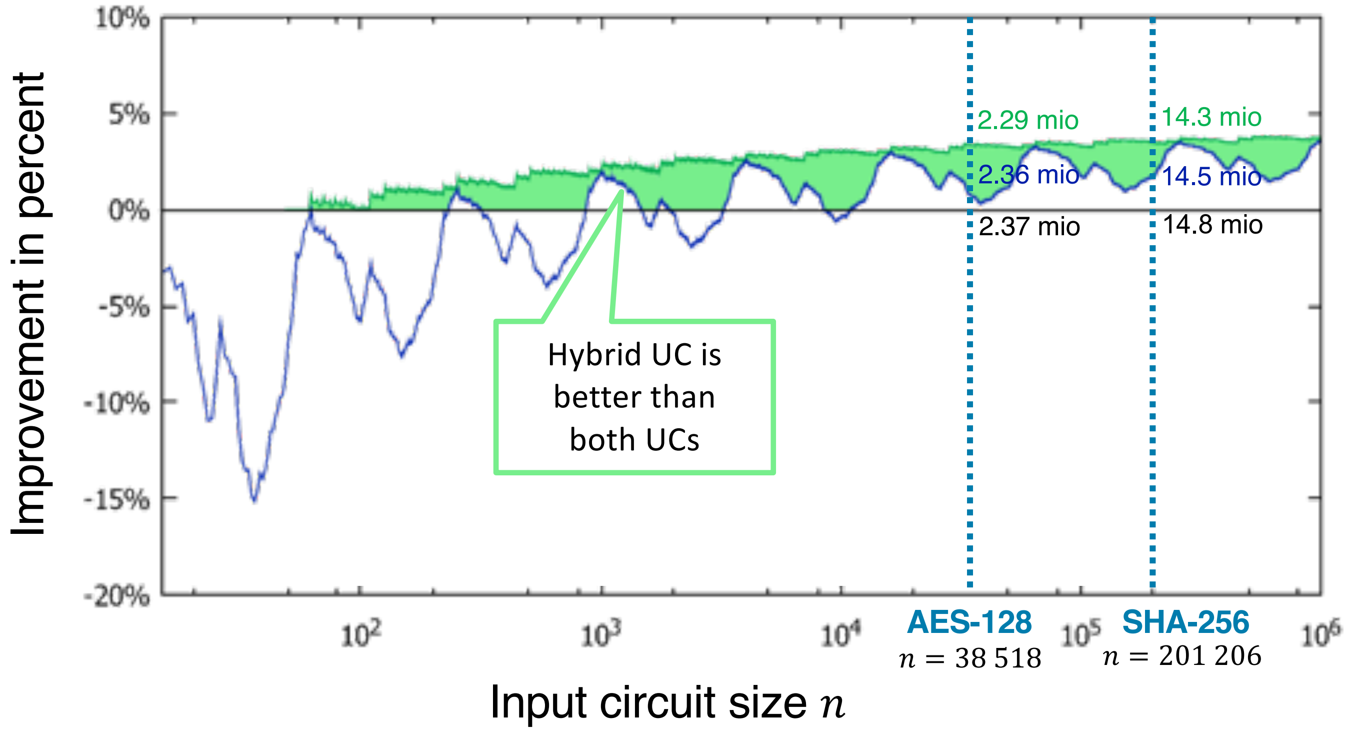
4-way split $\overset{?}{<>}$ 2-way split

⇨ At each recursion step: choose smallest construction

Concrete Size of UCs – Hybrid UC

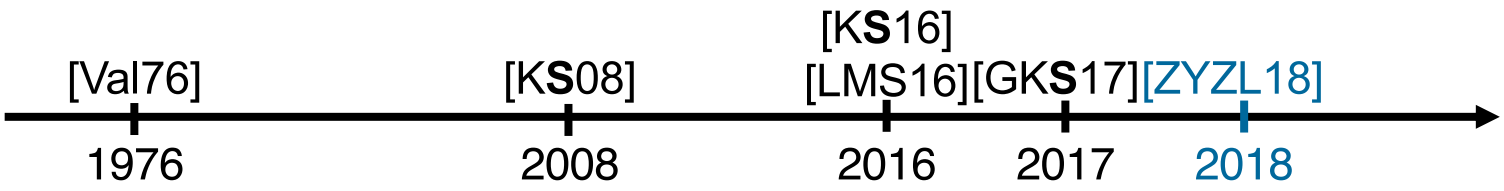
Green: Improvement of hybrid UC over 2-way UC

Blue: Improvement of 4-way UC over 2-way UC



Maximum: $\frac{5}{4.75} - 100\% = 5.3\%$

Existing UC Constructions

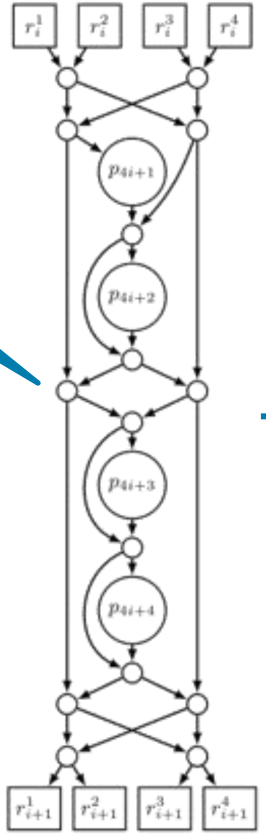


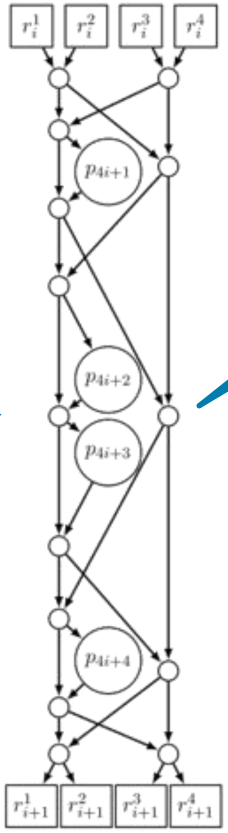
	[Val76] 2-way	[Val76] 4-way	[KS08]	[GKS17] Hybrid(2, 4)
Size	$5n \log n$	~~$4.75n \log n$~~ $4.5n \log n$	$1.5n \log^2 n + 2n \log n$	~~$4.75n \log n$~~ $4.5n \log n$
Depth	$3n$	~~$3.75n$~~ $3.5n$	$n \log n$	~~$3.75n$~~ $3.5n$
Code	✓	✗	✓	✗

[ZYZL18] S. Zhao, Y. Yu, J. Zhang and H. Liu: Valiant's Universal Circuits Revisited: An Overall Improvement and a Lower Bound. In *ePrint 2018/943;* to appear in *ASIACRYPT'19*.

Improved Block [ZYZL18]

15 additional nodes





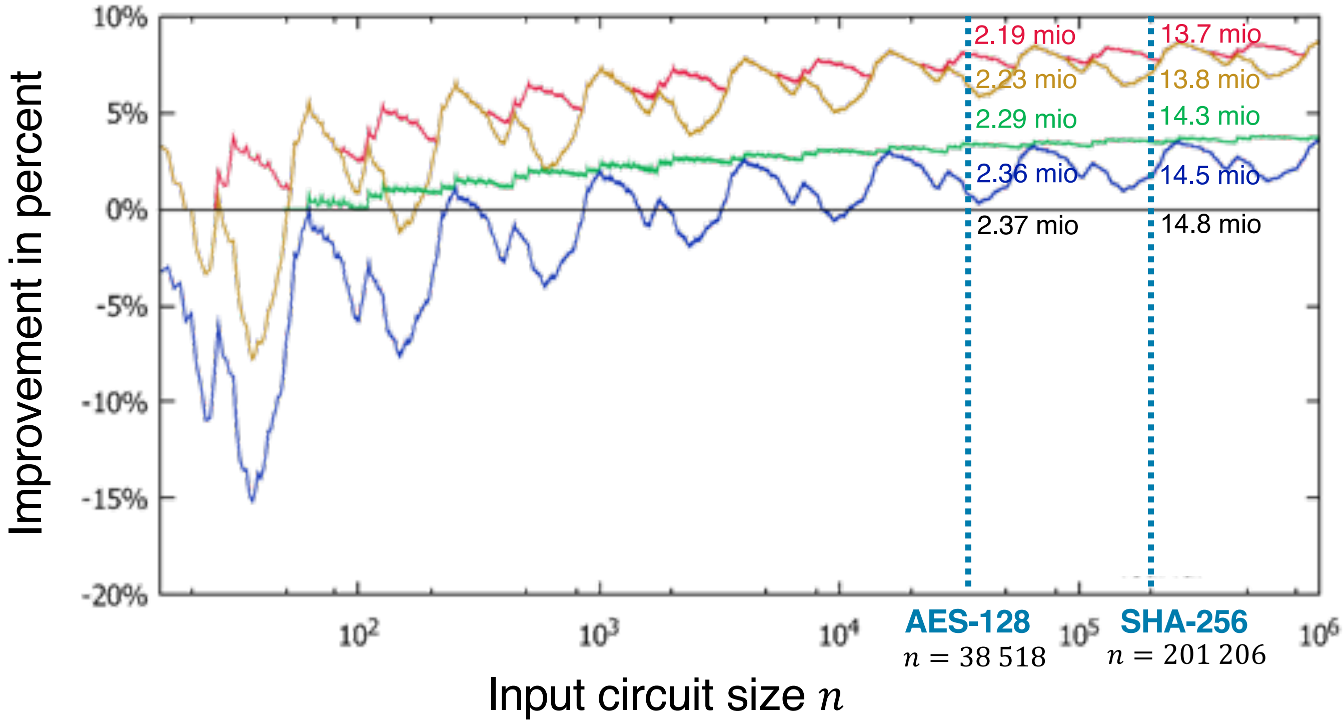
14 additional nodes

+ lower bound that this is optimal!

[ZYZL18] S. Zhao, Y. Yu, J. Zhang and H. Liu: Valiant's Universal Circuits Revisited: An Overall Improvement and a Lower Bound. In *ePrint 2018/943;* to appear in ASIACRYPT’19.

Concrete Size of UCs – Improvement of [ZYZL18]

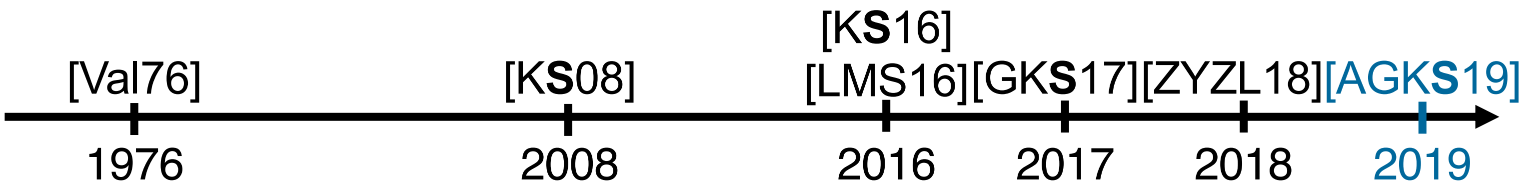
Red: Improvement of hybrid UC with [ZYZL18] 4-way UC over 2-way UC
Yellow: Improvement of [ZYZL18] 4-way UC over 2-way UC
Green: Improvement of hybrid UC over 2-way UC
Blue: Improvement of 4-way UC over 2-way **UC**



Maximum: $\frac{5}{4.5} - 100\% = 11.1\%$

Maximum: $\frac{5}{4.75} - 100\% = 5.3\%$

Existing UC Constructions

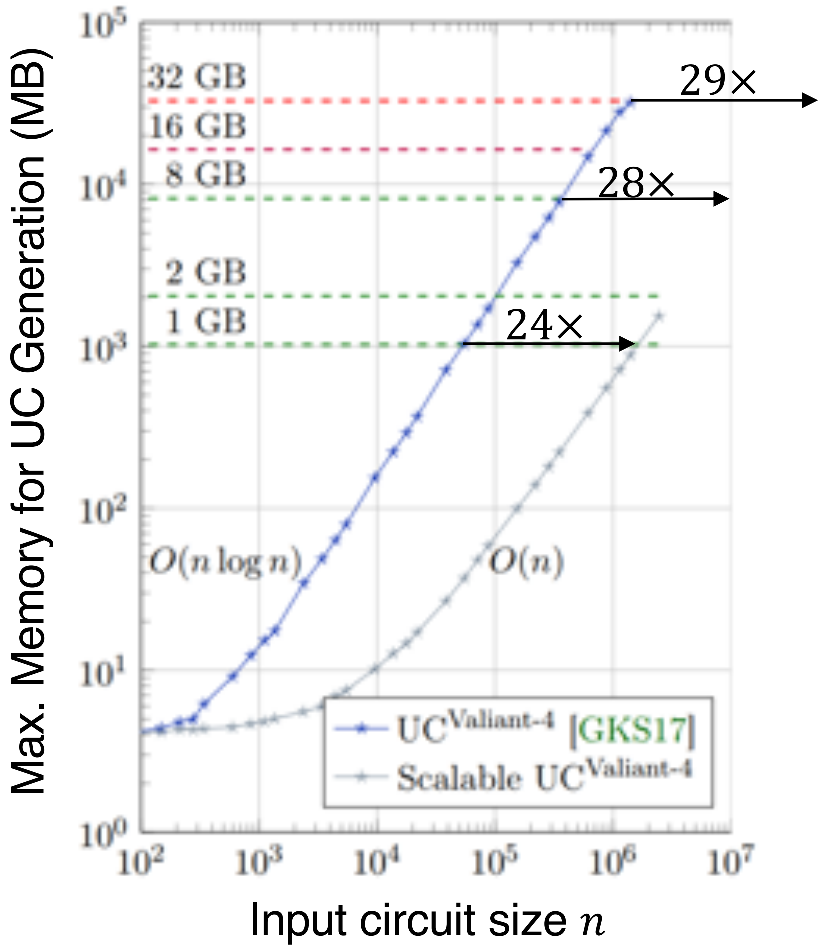


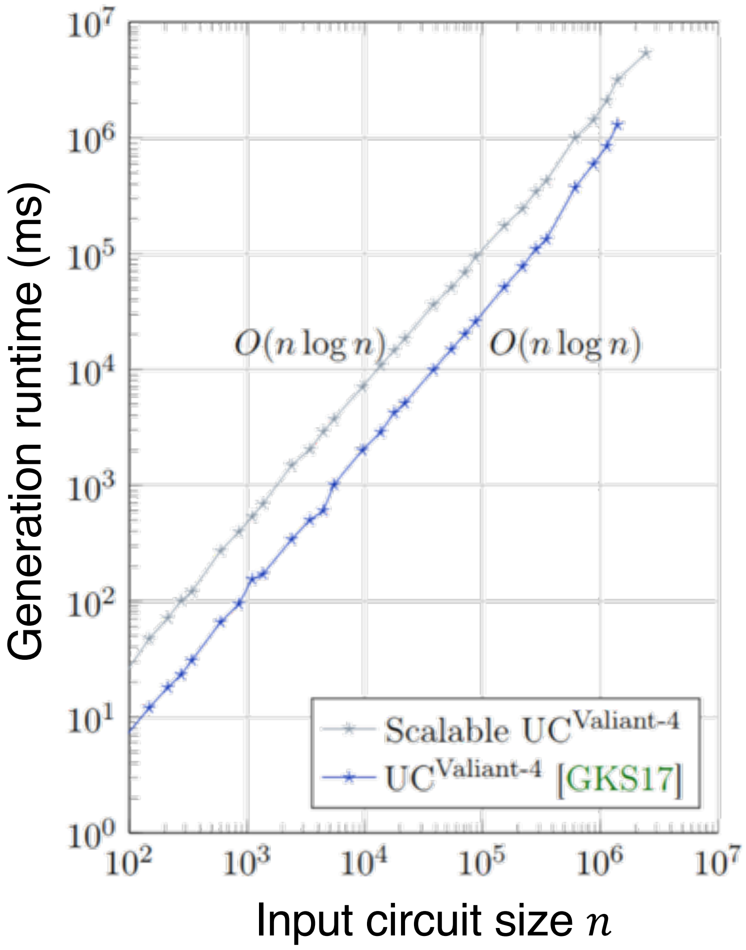
	[Val76] 2-way	[Val76] 4-way	[KS08]	[GKS17] Hybrid(2, 4)
Size	$5n \log n$	~~$4.75n \log n$~~ $4.5n \log n$	$1.5n \log^2 n$ $+ 2n \log n$	~~$4.75n \log n$~~ $4.5n \log n$
Depth	$3n$	~~$3.75n$~~ $3.5n$	$n \log n$	~~$3.75n$~~ $3.5n$
Code	✓	✓	✓	✓

+ Scalability

[AGK**S**17] M. Y. Alhassan, D. Günther, Á. Kiss, T. Schneider: Efficient and Scalable Universal Circuits. In *ePrint 2019/348*; in submission.

Scalable 4-way UC Implementation





UC Implementation

[MNPS04]

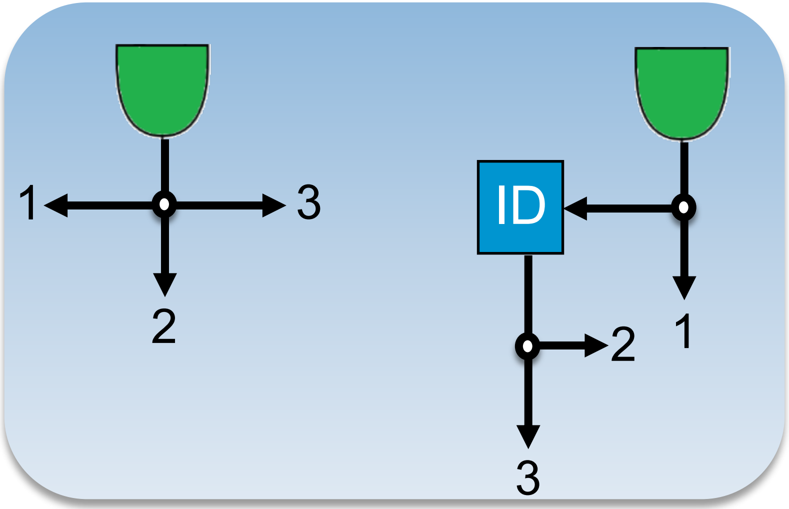
C_0 ◄···· f SHDL

[MNPS04] D. Malkhi, N. Nisan, B. Pinkas, Y. Sella. Fairplay-Secure Two-Party Computation System. In *USENIX Security'04.*

UC Implementation

[K**S**16]

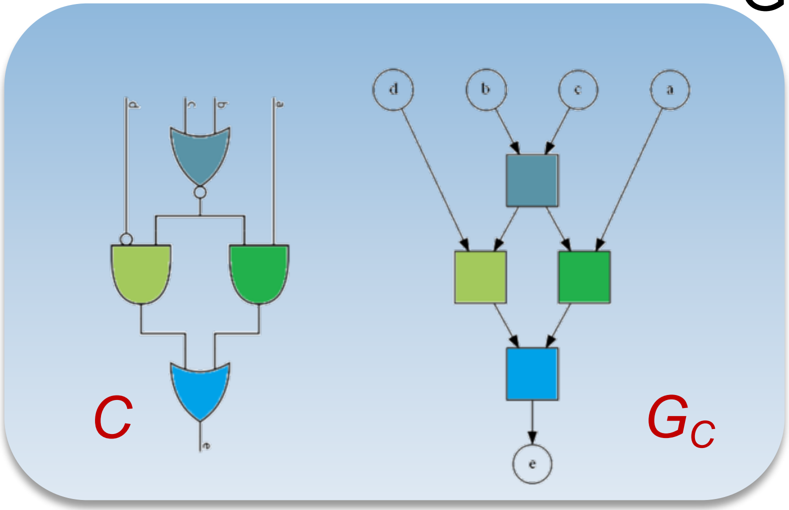
C size $\leq n$ ⟵ C_0 ⟵ f

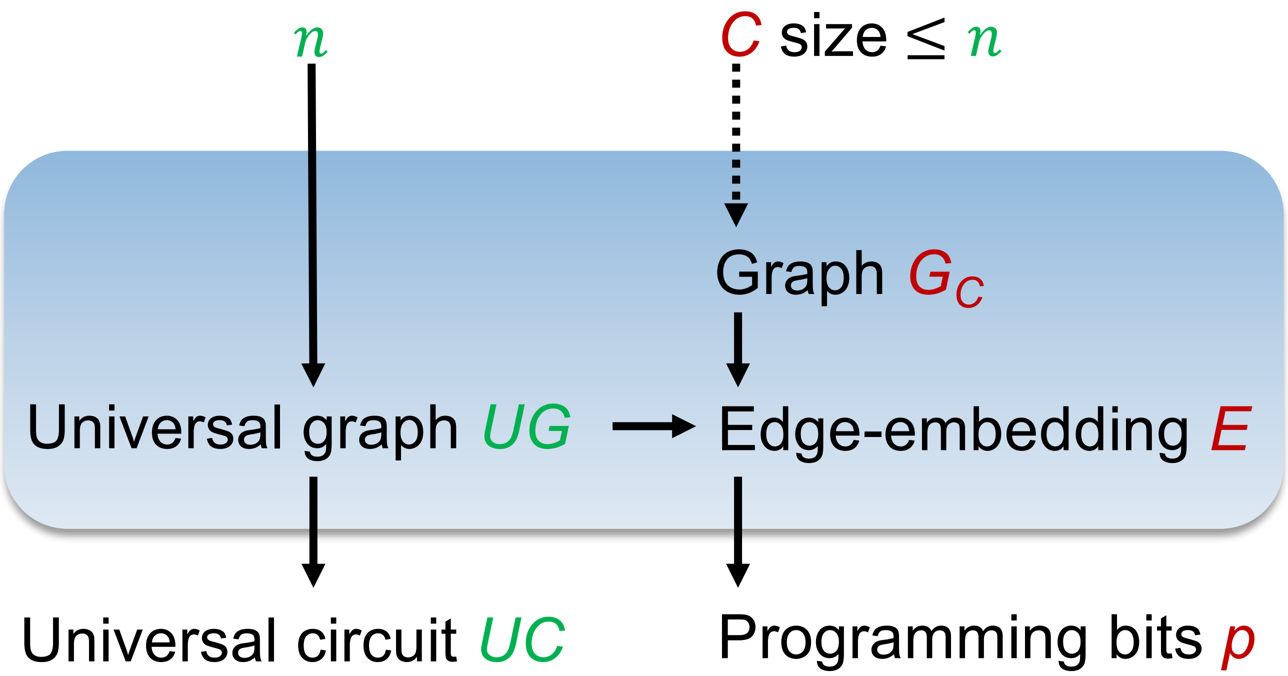


[K**S**16] Á. Kiss, T. Schneider: Valiant's Universal Circuit is Practical. In *EUROCRYPT'16.*

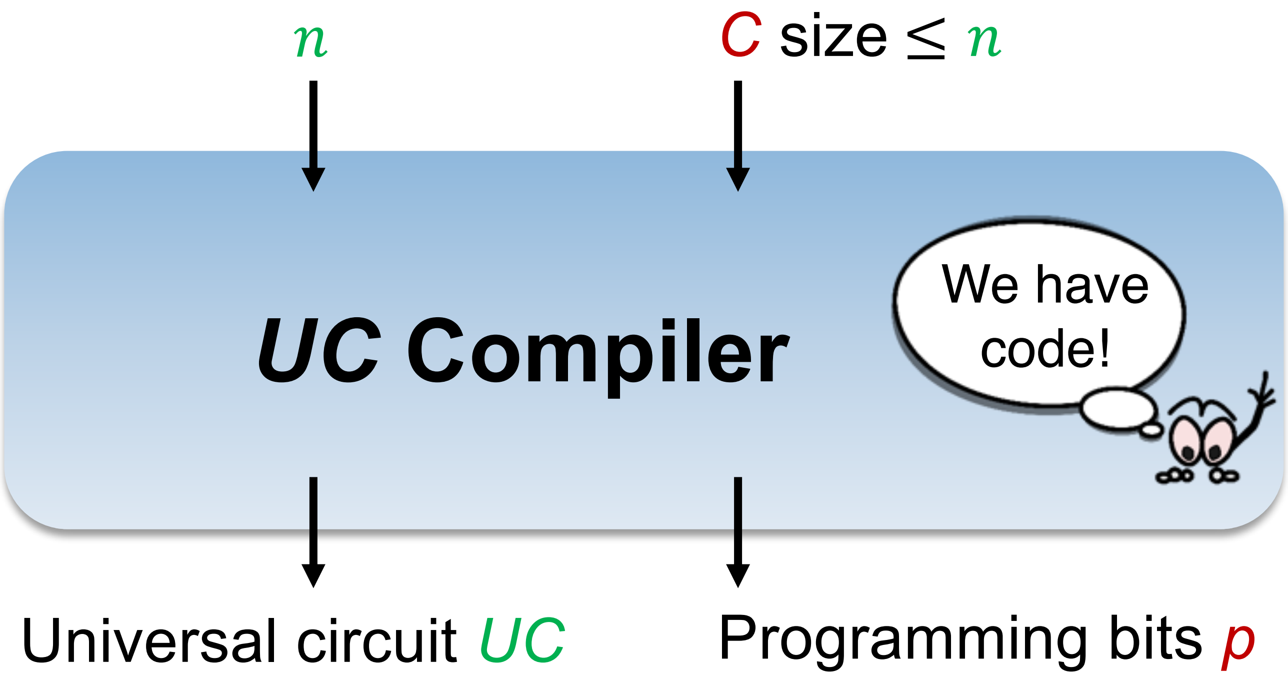
C size $\leq n$

Graph G_C



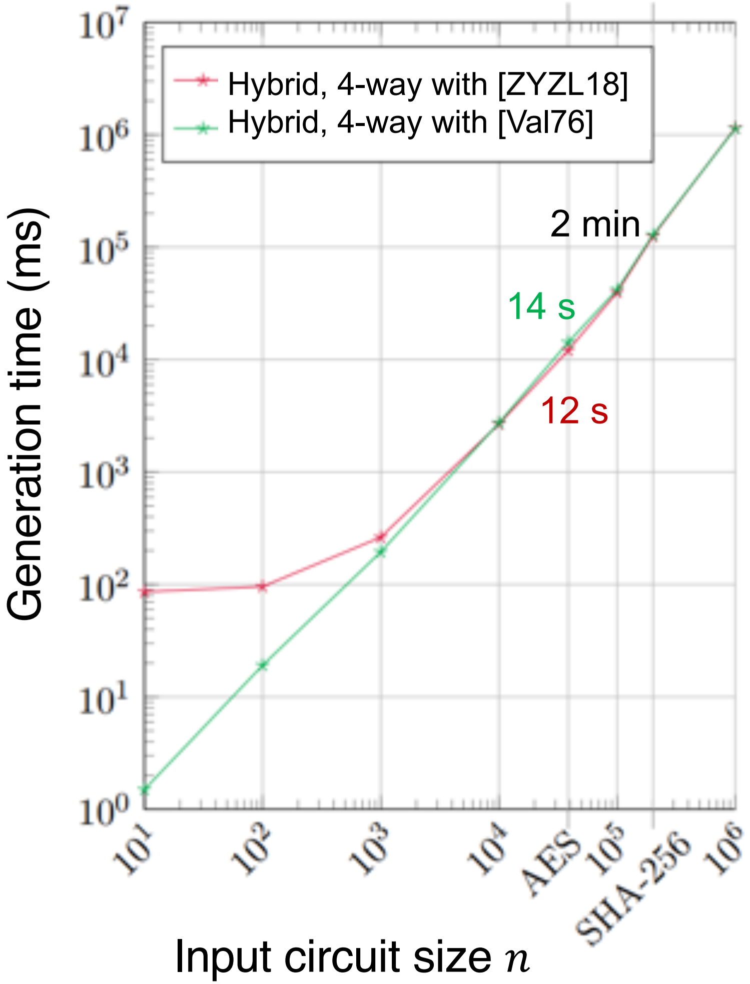

n
C size $\leq n$
Graph G_C
Universal graph UG
Edge-embedding E
Universal circuit UC
Programming bits p

UC Implementation

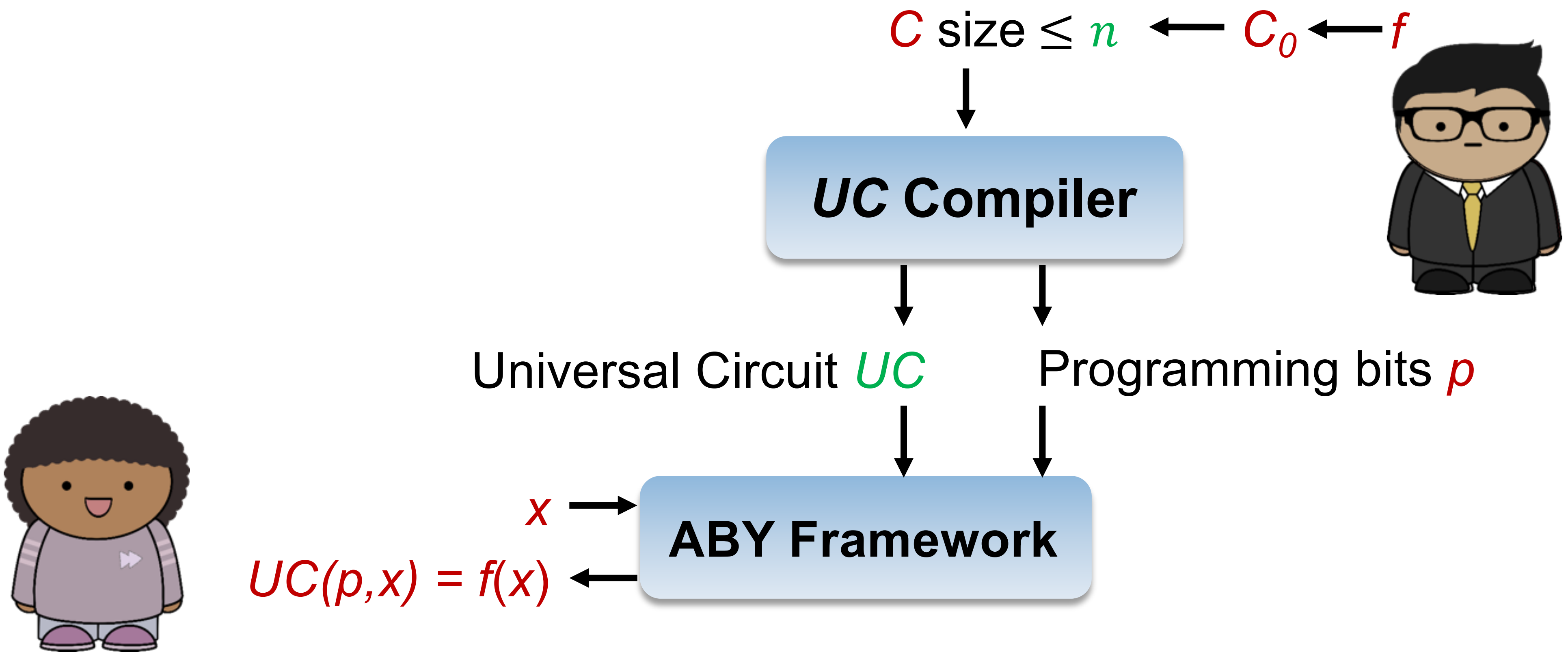


Code: https://encrypto.de/code/UC

Experimental Results – UC Compiler (one-time expense)

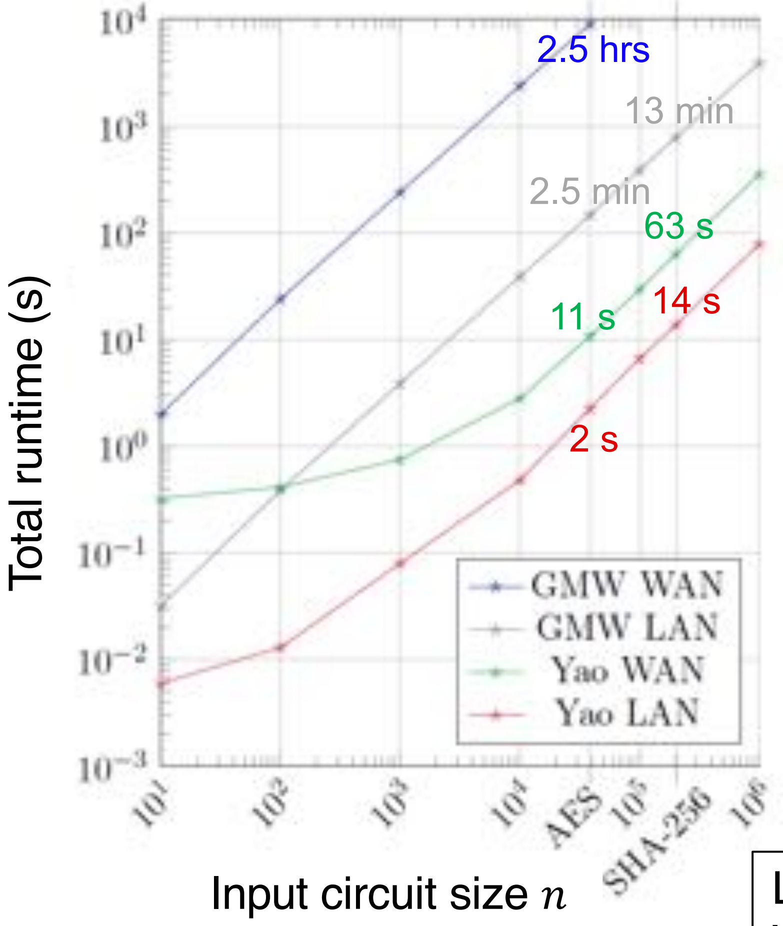


Implementation of PFE via UC

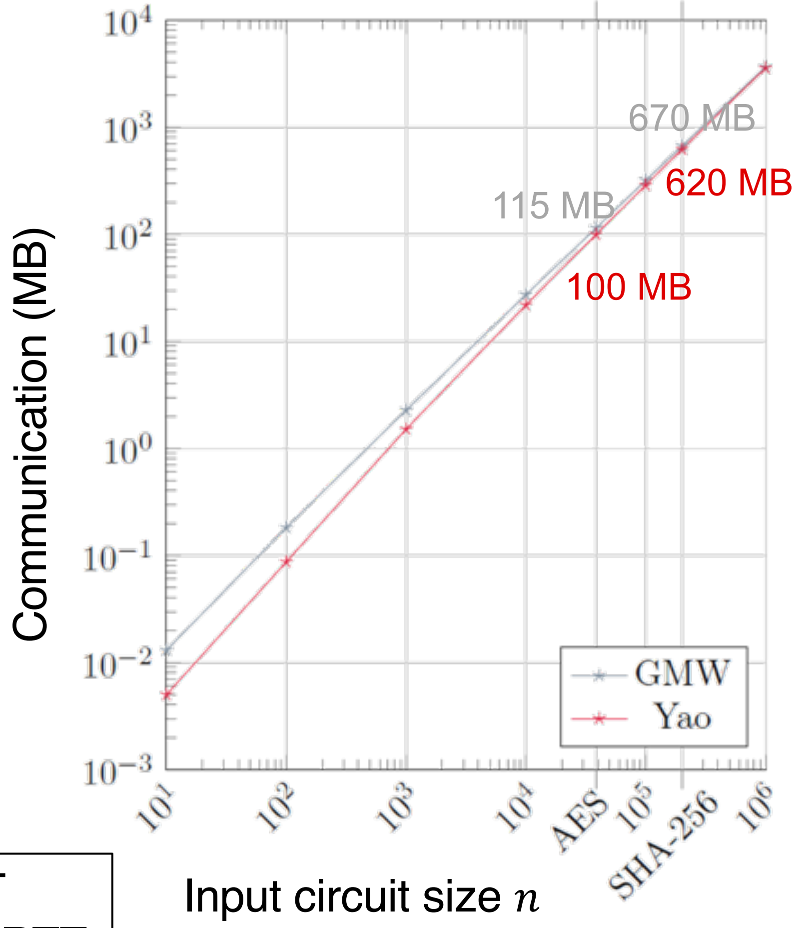


[DSZ15] D. Demmler, T. Schneider, M. Zohner. ABY – A Framework for Efficient Mixed-protocol Secure Two-party Computation. In *NDSS'15.*

Runtime and Communication for PFE of Boolean Circuits



LAN: 10 Gbps, 1ms RTT
WAN: 100Mbps, 100ms RTT



Conclusions for PFE of Boolean Circuits

- Universal Circuits are a competitive solution for PFE of Boolean Circuits
  - UC size has reached lower bound of $4.5n \log n$ AND gates for circuits of size n gates

- Performance of UC-based PFE (using Yao's GC in ABY):
  - AES ($n = 38\,518$): 2s in LAN; 11s in WAN
  - $n = 1\,000\,000$: 1.3 min in LAN; 5.9 mins in WAN

- Extending secure computation frameworks for PFE with UCs is simple
  - Simple adapter for UC format (similar to Fairplay's SHDL)
  - Code at https://encrypto.de/code/UC

Thanks for
your attention!

Questions?

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Contact: https://encrypto.de