Pushing the Limits of Valiant's Universal Circuits: Simpler, Tighter and More Compact

Hanlin Liu, Yu Yu, Shuoyao Zhao, Jiang Zhang, Wenling Liu and Zhenkai Hu

Shanghai Jiao Tong University

Shanghai Qi Zhi Institute

Shanghai Key Laboratory of Privacy-Preserving Computation

State Key Laboratory of Cryptology

Universal Circuits -- General-purpose Circuits

- **Universal Circuit** UC_n

  for any $|C| \leq n$, $\exists p_C \in \{0,1\}^m$, s.t.,

  $$\forall x: UC_n\ (x, p_C) = C(x).$$

- **Theorem** [Valiant76]: There exists explicit universal circuit $\boldsymbol{UC}$ that simulates any $\boldsymbol{C}$ with
  - size up to $\boldsymbol{n}$
  - fan-in and fan-out 2

  where UC is represented by an edge-universal-graph (EUG) on graph and

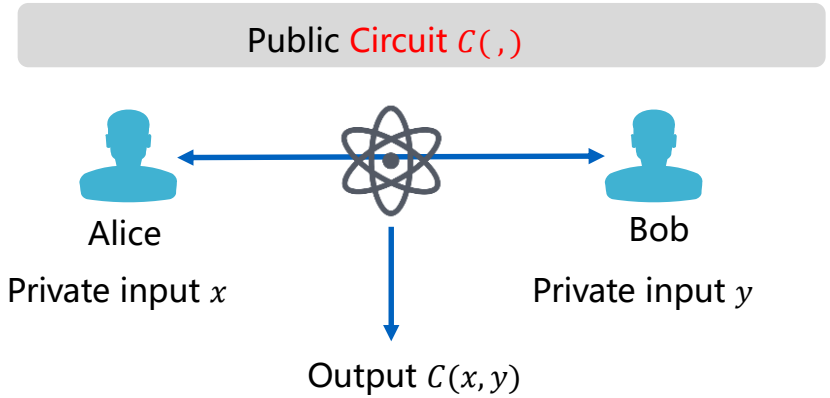
  $$\text{Size}(EUG) \sim 4.75n \log n, \quad \text{Size}(UC) \sim 19n \log n\,.$$

- **State-of-the-art**: $3.64n \log n \leq Size(EUG) \leq 4.5n \log n$ in Valiant' framework

  our work: $2.95n \log n \leq Size(EUG) \leq 3n \log n$

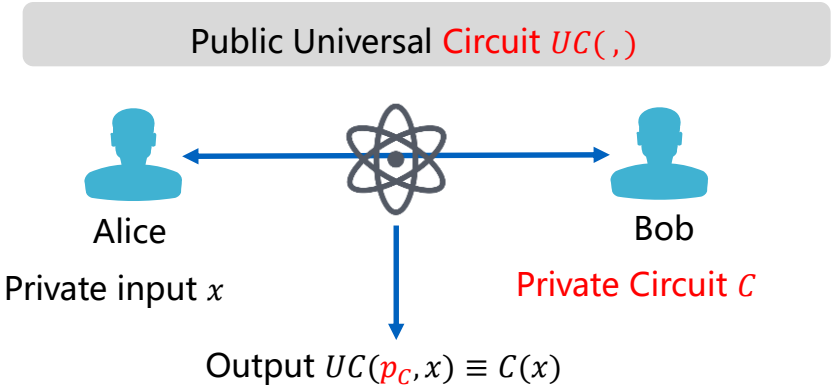
Application in Multiparty Computation

- Multiparty Computation preserves input privacy



- Q: Function privacy? e.g., Bob holds private circuit C

  A: Universal Circuits



Edge Embedding and Edge Universal Graphs

Edge-Embedding:

injective map ρ: $G = (V, E) \rightarrow G^* = (V^*, E^*)$, s.t.,

- $V \rightarrow V^*$
- $(v_i, v_j) \in E \rightarrow$ path $(\rho(v_i), \ldots, \rho(v_j)) \in E^*$

Edge-Universal Graphs (EUG):

- G^* is $EUG_d(n)$

  $\Leftrightarrow$ for any $G \in DAG_d(n)$, $\exists \rho$: $G \rightarrow G^*$

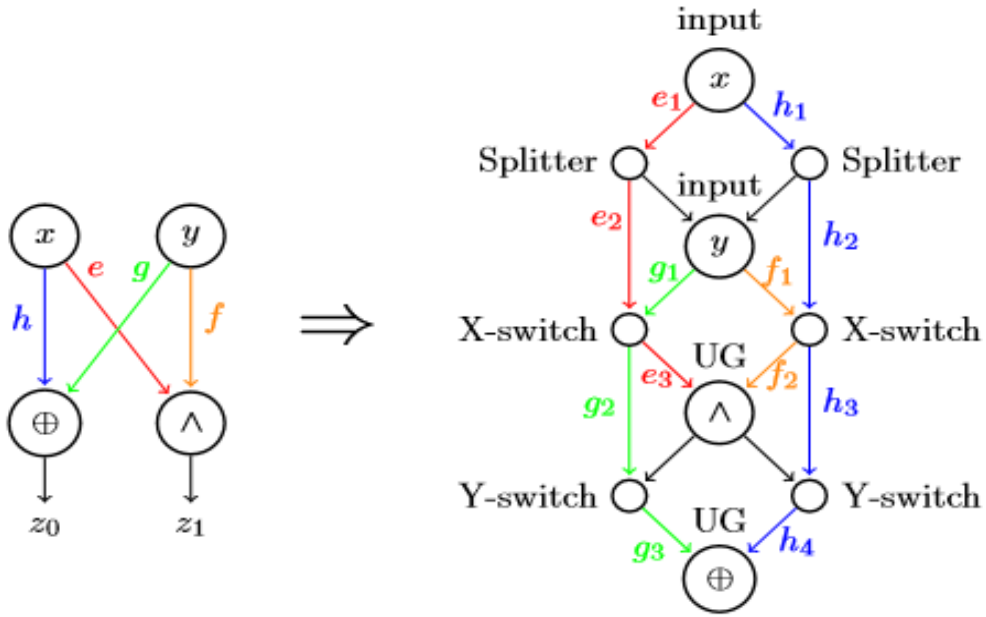
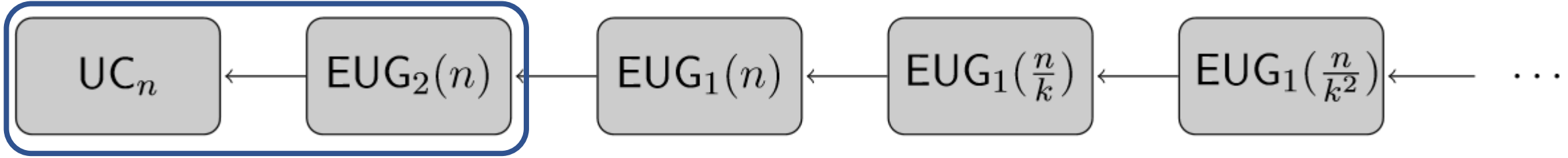
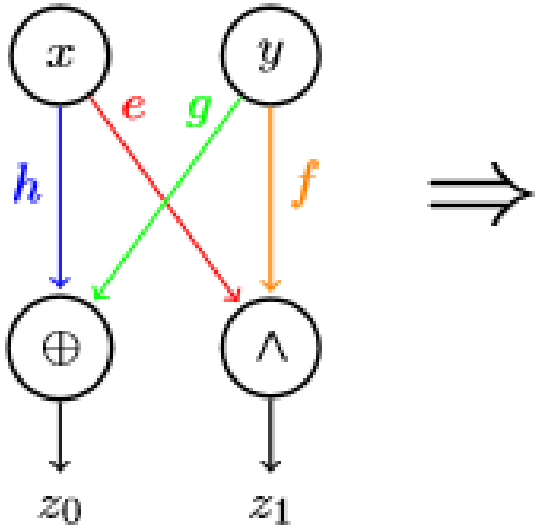
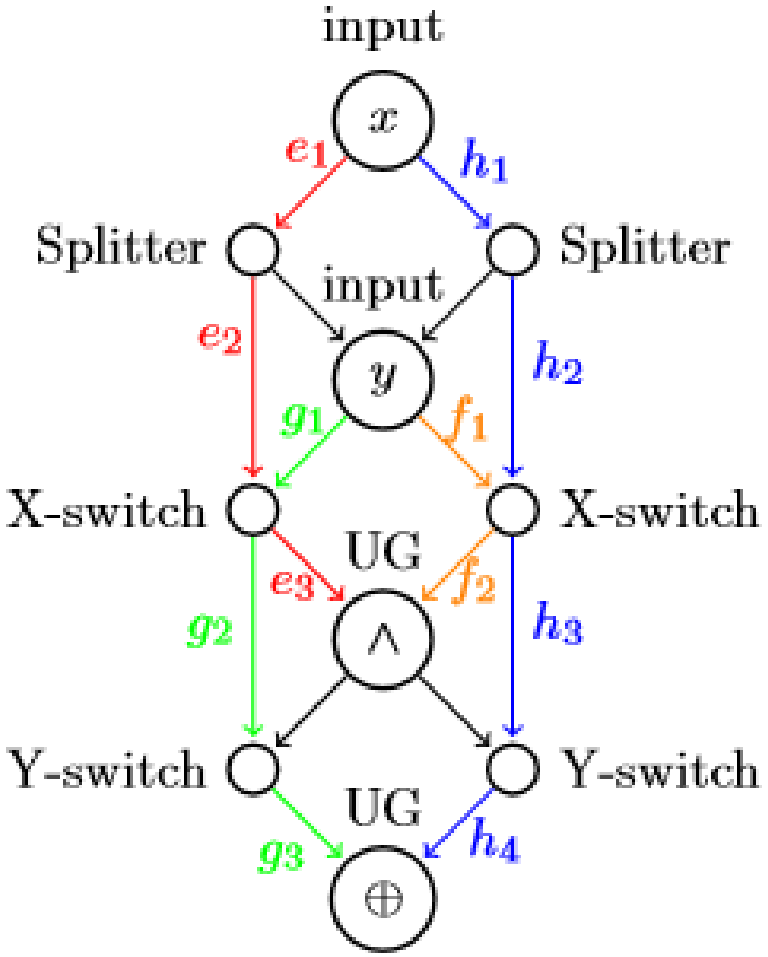


Fig. 2. An example of edge-embedding.

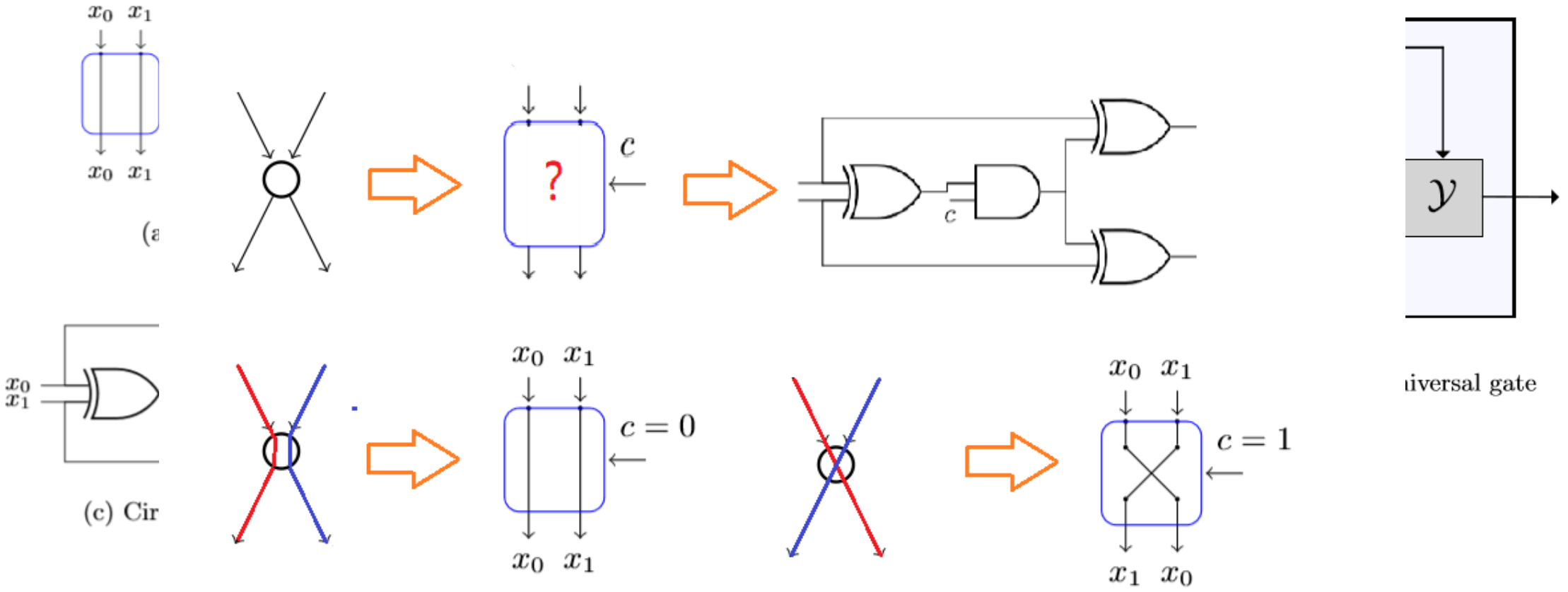

UC_n
$\mathsf{EUG}_2(n)$
$\mathsf{EUG}_1(n)$
$\mathsf{EUG}_1(\frac{n}{k})$
$\mathsf{EUG}_1(\frac{n}{k^2})$
$\cdots$

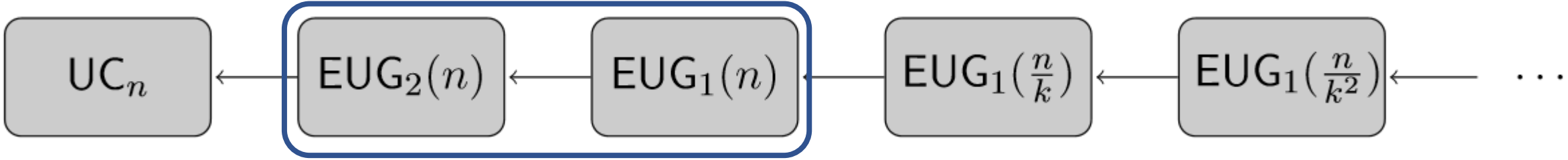

x
y
e
g
h
f
$\oplus$
$\wedge$
z_0
z_1


input
x
e_1
h_1
Splitter
Splitter
input
e_2
y
h_2
g_1
f_1
X-switch
X-switch
UG
e_3
f_2
g_2
$\wedge$
h_3
Y-switch
Y-switch
UG
g_3
h_4
$\oplus$

Switching Gates and Universal Gates

- X-switching gate = 4 basic gates (AND and XOR)
- Y-switching gate = 3 basic gates
- Universal gate = 3 Y-switching gates

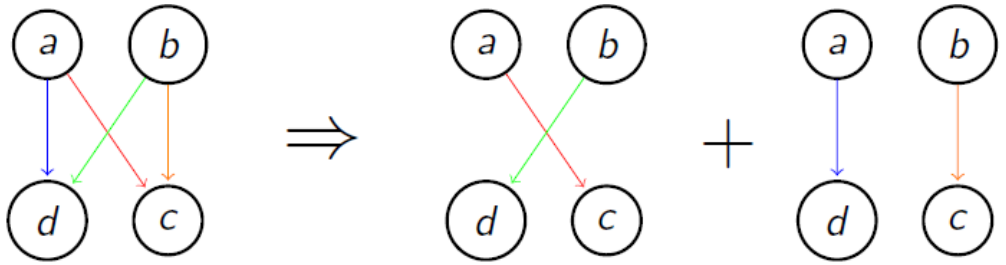


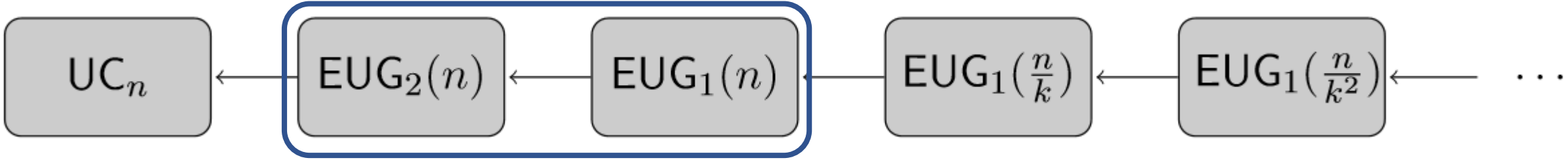


[**Valiant76**] For any graph $G = (V, E) \in DAG_d(n)$, edge set E can be divided into d disjoint sets $E_1, E_2, \cdots, E_d$ such that

$$E = \cup_{i=1}^{d} E_i$$

and each $(V, E_i) \in DAG_1(n)$ for $1 \leq i \leq d$.

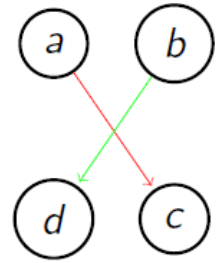


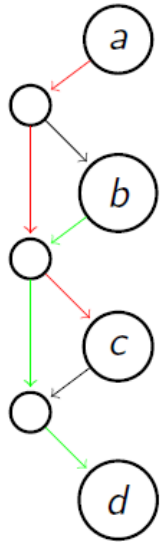


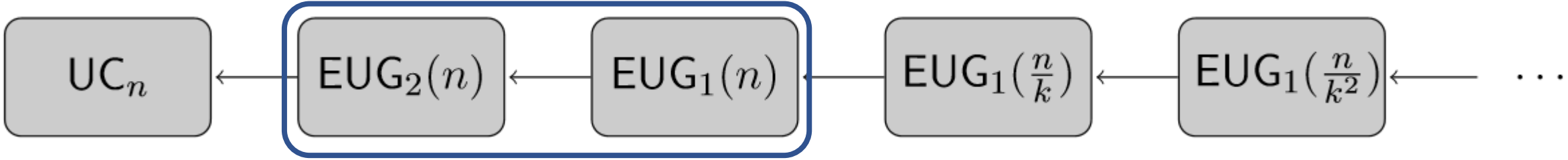
[**Valiant76**] For any graph $G = (V, E) \in DAG_d(n)$, edge set E can be divided into d disjoint sets $E_1, E_2, \cdots, E_d$ such that

$$E = \cup_{i=1}^{d} E_i$$

and each $(V, E_i) \in DAG_1(n)$ for $1 \leq i \leq d$.



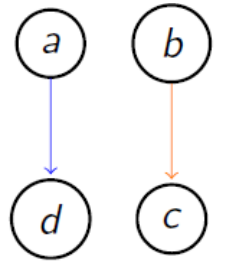


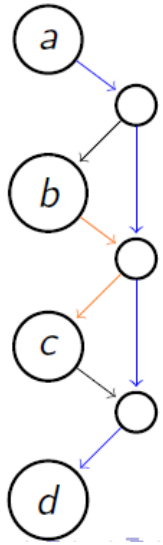


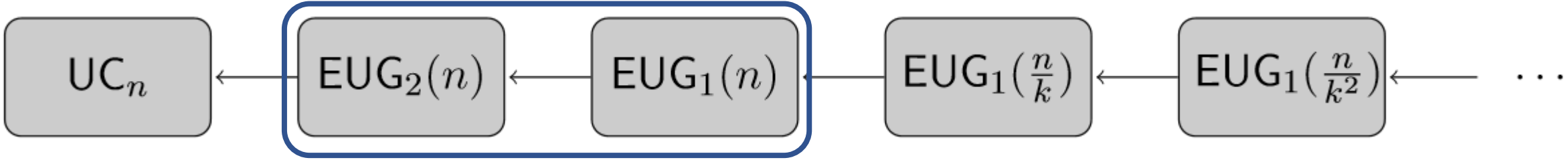
[**Valiant76**] For any graph $G = (V, E) \in DAG_d(n)$, edge set E can be divided into d disjoint sets $E_1, E_2, \cdots, E_d$ such that

$$E = \cup_{i=1}^{d} E_i$$

and each $(V, E_i) \in DAG_1(n)$ for $1 \leq i \leq d$.



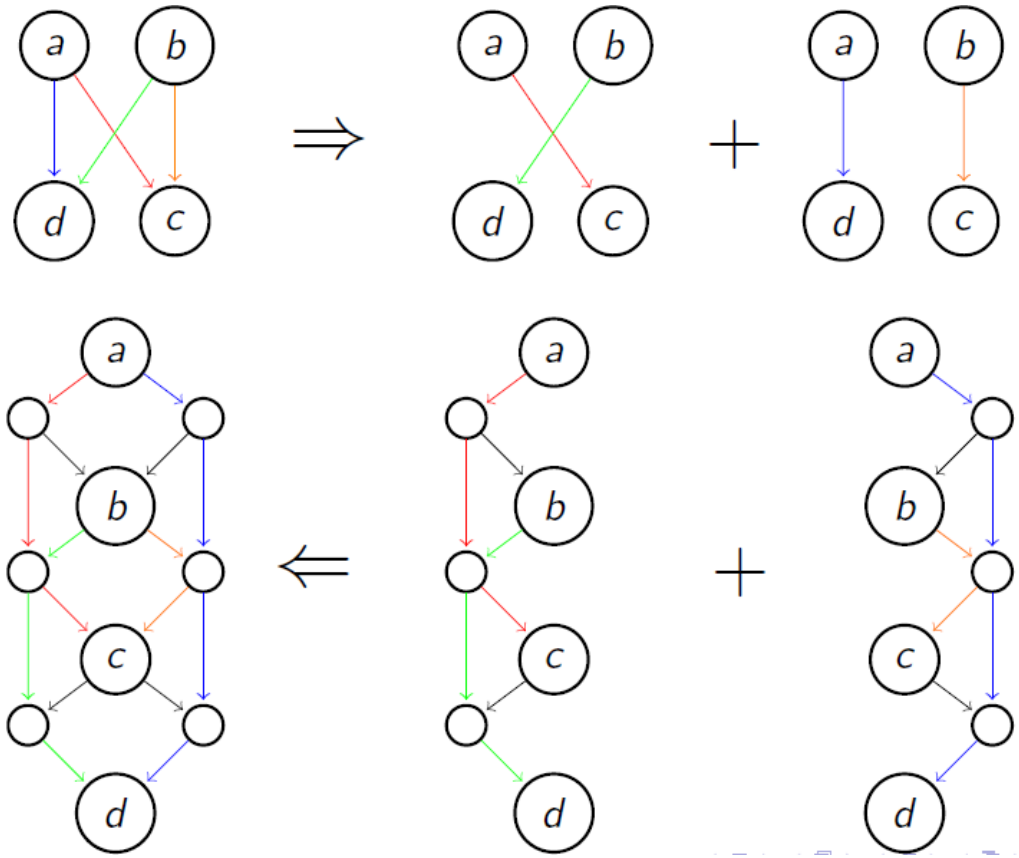


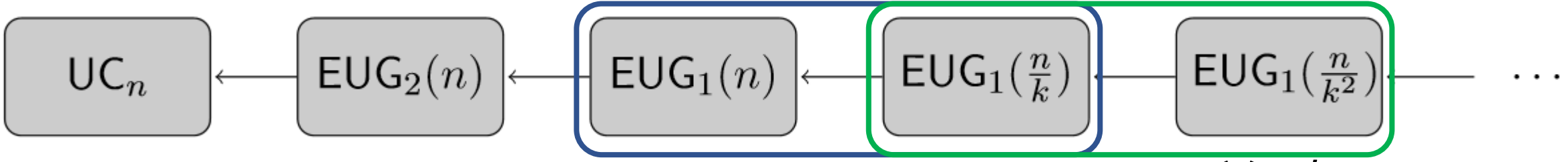


[**Valiant76**] For any graph $G = (V, E) \in DAG_d(n)$, edge set E can be divided into d disjoint sets $E_1, E_2, \cdots, E_d$ such that

$$E = \cup_{i=1}^{d} E_i$$

and each $(V, E_i) \in DAG_1(n)$ for $1 \leq i \leq d$.



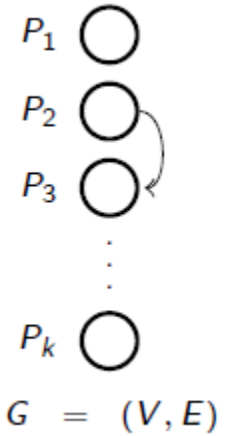


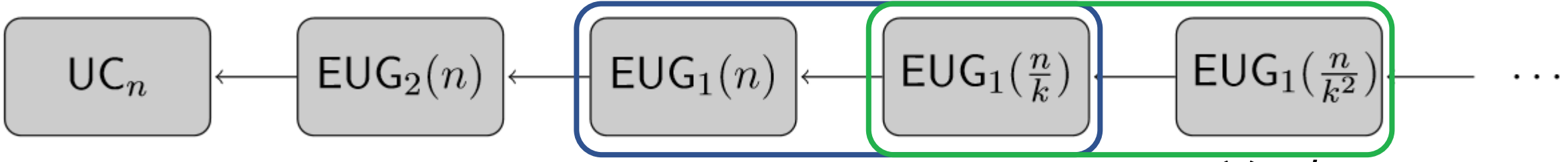
- **Definition 1** (Augmented DAG) for any graph $\mathrm{G} = (\mathrm{V}, \mathrm{E}) \in \mathrm{DAG}_1(\mathrm{k})$, $\mathrm{G}' = (\mathrm{V}', \mathrm{E}') \in \mathrm{DAG}_1\ (3\mathrm{k})$ is the augmented DAG of G if

$$\mathrm{V}' = \{in_1, \dots, in_k\} \cup \mathrm{V} \cup \{out_1, \dots, out_k\}$$

$$\mathrm{E}' = \mathrm{E} \cup E_{aux}$$

every $\mathrm{e} \in E_{aux}$: either $\mathrm{e} = (\mathrm{in}_{\mathrm{i}_1}, \mathrm{p}_{\mathrm{j}_1})$ or $\mathrm{e} = (\mathrm{p}_{\mathrm{i}_2}, \mathrm{out}_{\mathrm{j}_2})$.



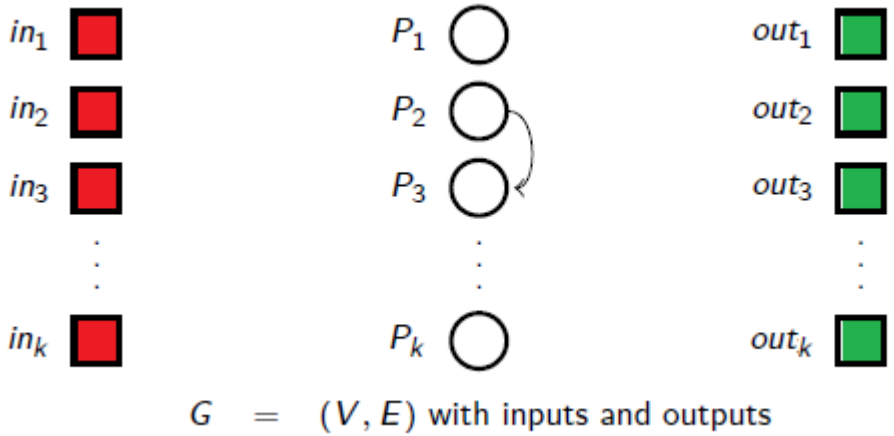


- **Definition 1** (Augmented DAG) for any graph $G = (V, E) \in DAG_1(k)$, $G' = (V', E') \in DAG_1(3k)$ is the augmented DAG of G if

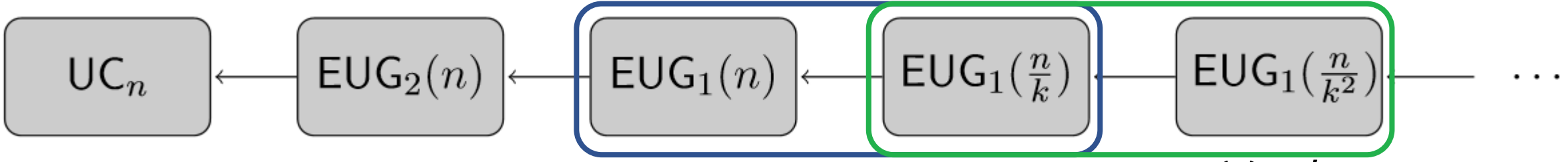
$$V' = \{in_1, \dots, in_k\} \cup V \cup \{out_1, \dots, out_k\}$$

$$E' = E \cup E_{aux}$$

every $e \in E_{aux}$: either $e = (in_{i_1}, p_{j_1})$ or $e = (p_{i_2}, out_{j_2})$.



$G = (V, E)$ with inputs and outputs

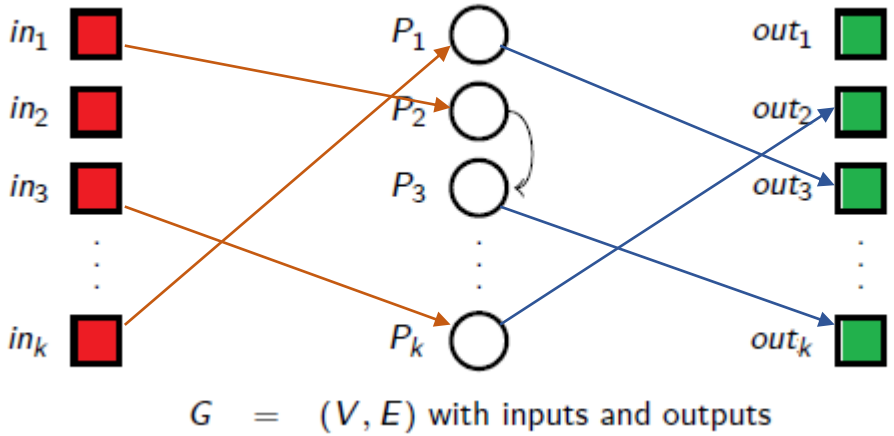


- **Definition 1** (Augmented DAG) for any graph $G = (V, E) \in DAG_1(k)$, $G' = (V', E') \in DAG_1\ (3k)$ is the augmented DAG of G if

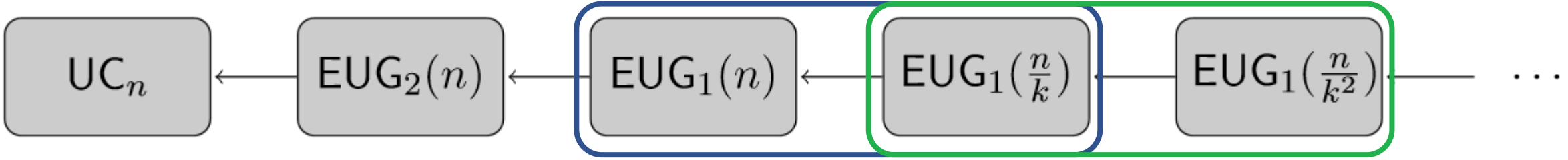
$$V' = \{in_1, \dots, in_k\} \cup V \cup \{out_1, \dots, out_k\}$$

$$E' = E \cup E_{aux}$$

every $e \in E_{aux}$: either $e = (in_{i_1}, p_{j_1})$ or $e = (p_{i_2}, out_{j_2})$.

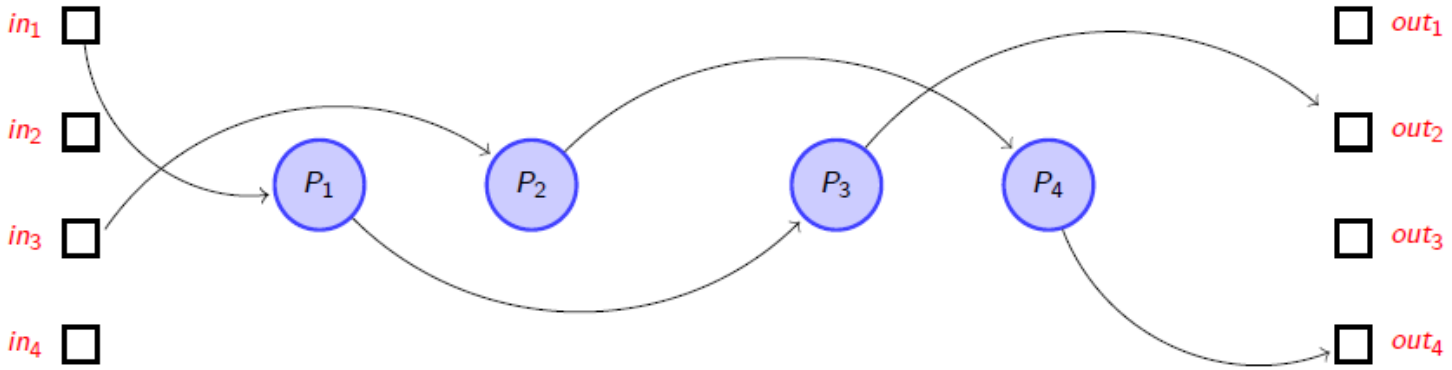


$G = (V, E)$ with inputs and outputs

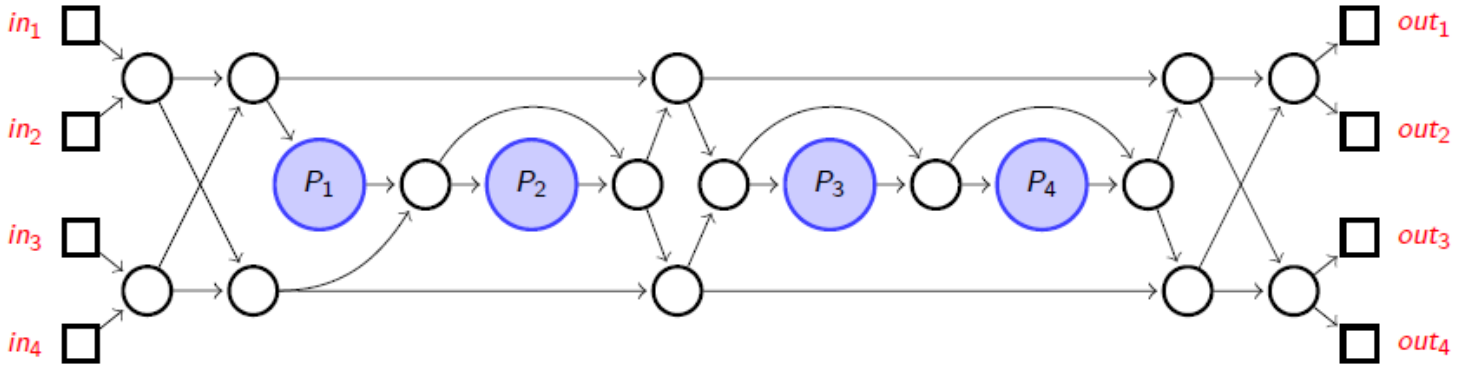


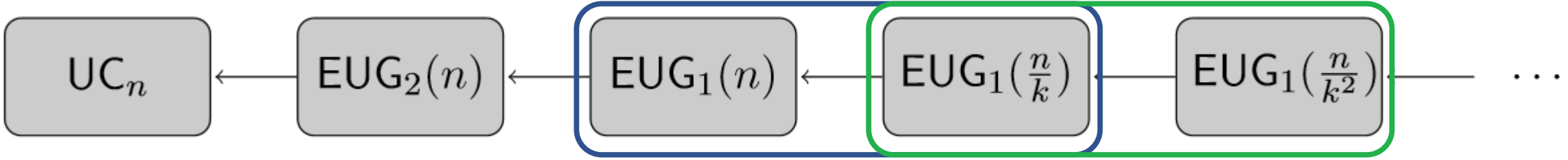
- **Definition 2** (k-way Supernode, denoted by SN(k)): edge-universal graphs for Augmented $\mathrm{DAG}_1(\mathrm{k})$.

Augmented $\mathrm{DAG}_1(4)$:



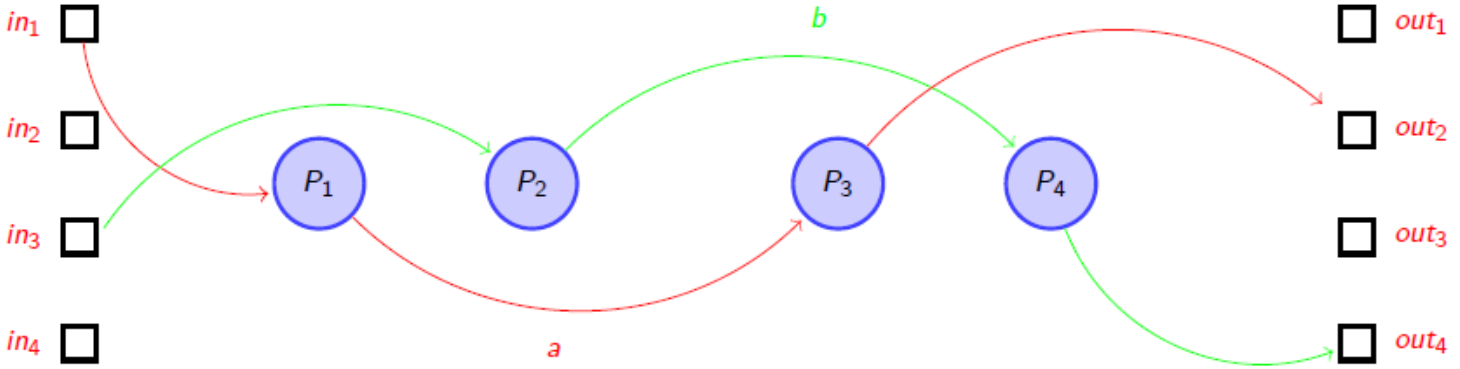
$\mathrm{SN}(4)$:



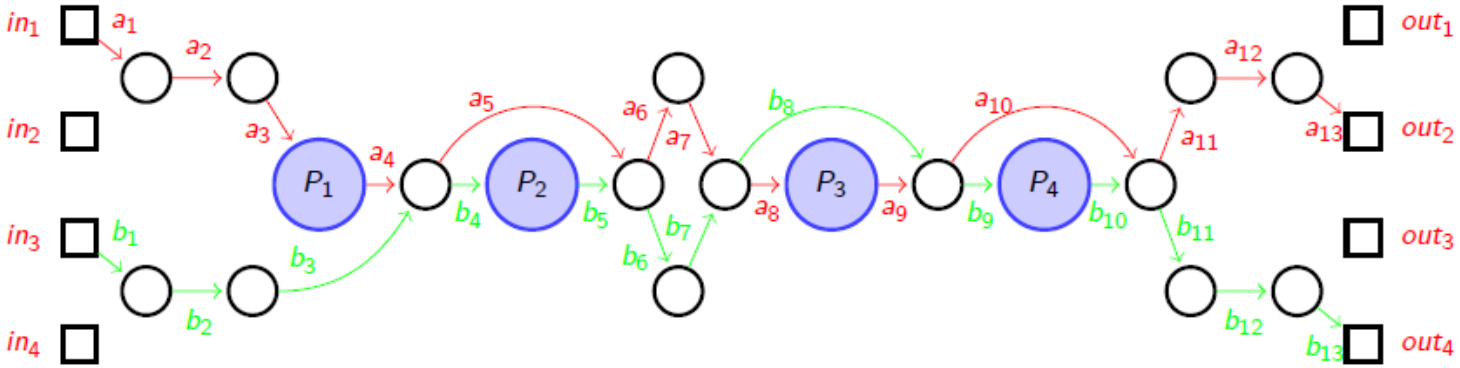


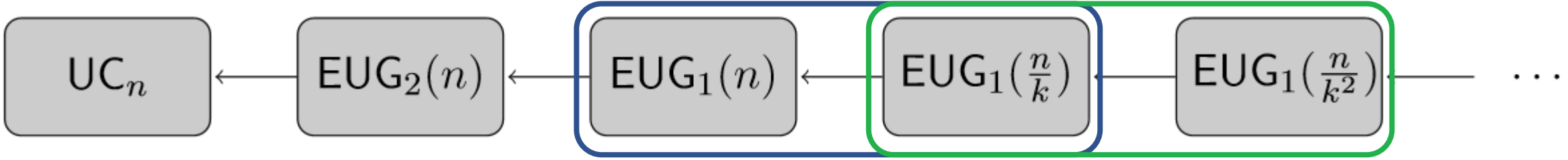
- **Definition 2** (k-way Supernode, denoted by SN(k)): edge-universal graphs for Augmented $\mathrm{DAG}_1(\mathrm{k})$.

Augmented $\mathrm{DAG}_1(4)$:

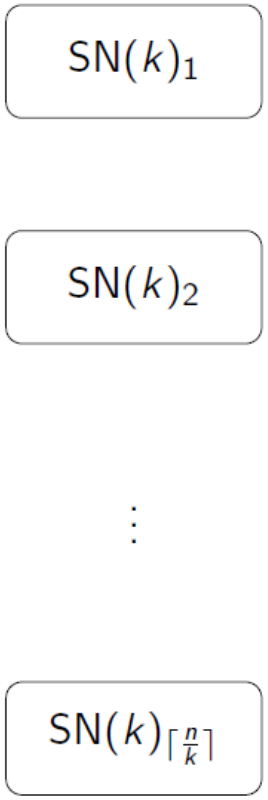


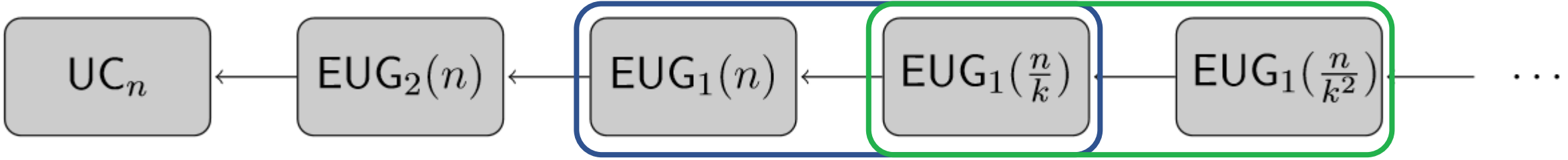
$\mathrm{SN}(4)$:



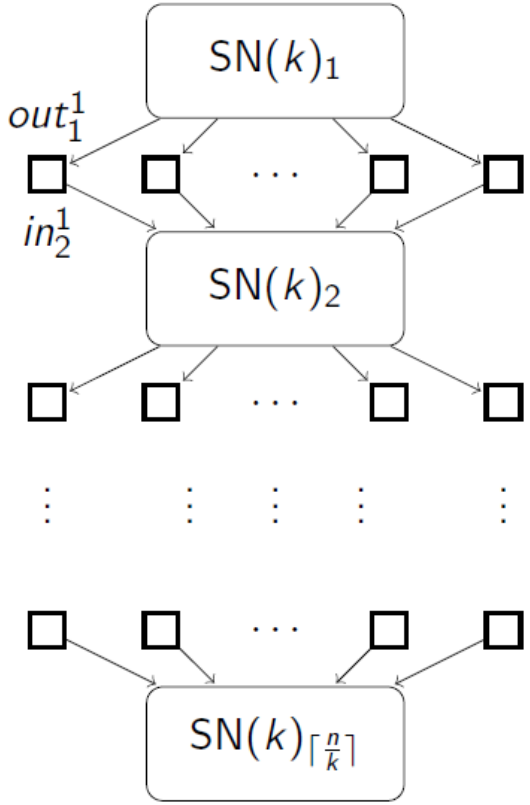


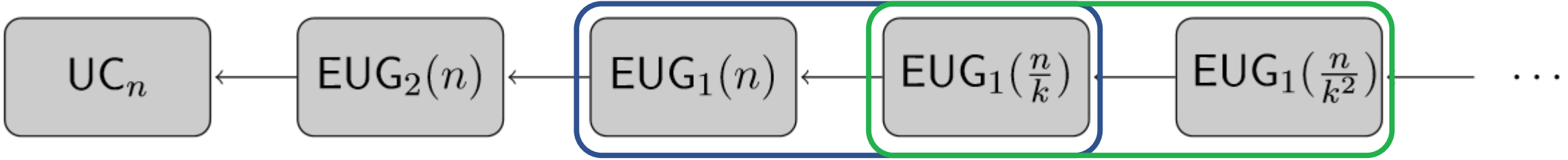
[**Valiant76**]: $\mathrm{EUG}_1(\lceil n/k \rceil - 1)$ + k-way supernode $\mathrm{SN(k)} \rightarrow \mathrm{EUG}_1(\mathrm{n})$, then we have $|\mathrm{EUG}_1(\mathrm{n})| = \mathrm{k} \cdot |\mathrm{EUG}_1(\lceil n/k \rceil - 1)| + \lceil n/k \rceil \cdot |\mathrm{SN}\ (\mathrm{k})|$



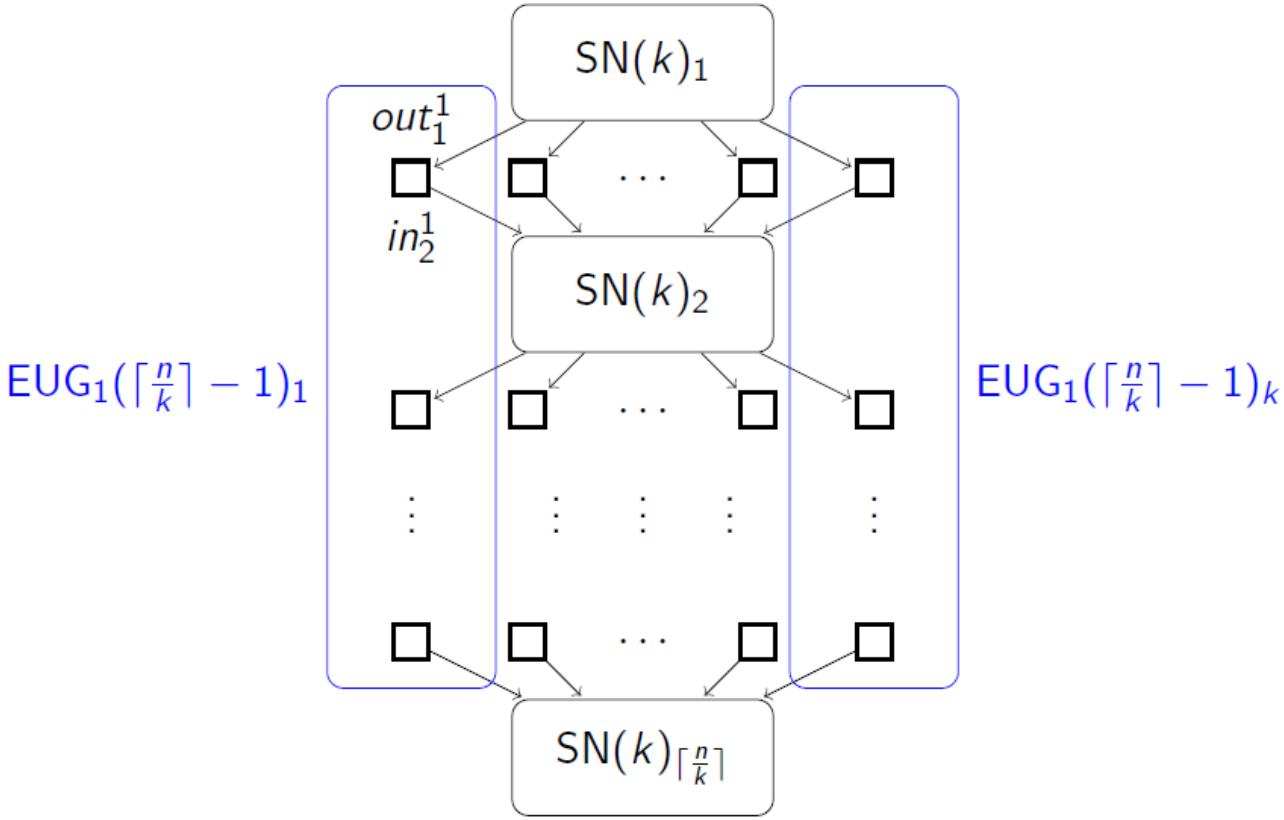


[**Valiant76**]: $\mathrm{EUG}_1(\lceil n/k \rceil - 1)$ + k-way supernode $\mathrm{SN(k)} \rightarrow \mathrm{EUG}_1(\mathrm{n})$, then we have $|\mathrm{EUG}_1(\mathrm{n})| = \mathrm{k} \cdot |\mathrm{EUG}_1(\lceil n/k \rceil - 1)| + \lceil n/k \rceil \cdot |\mathrm{SN}\ (\mathrm{k})|$

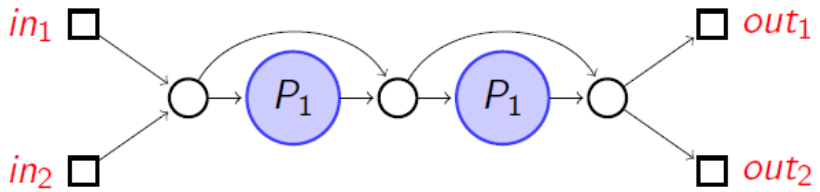




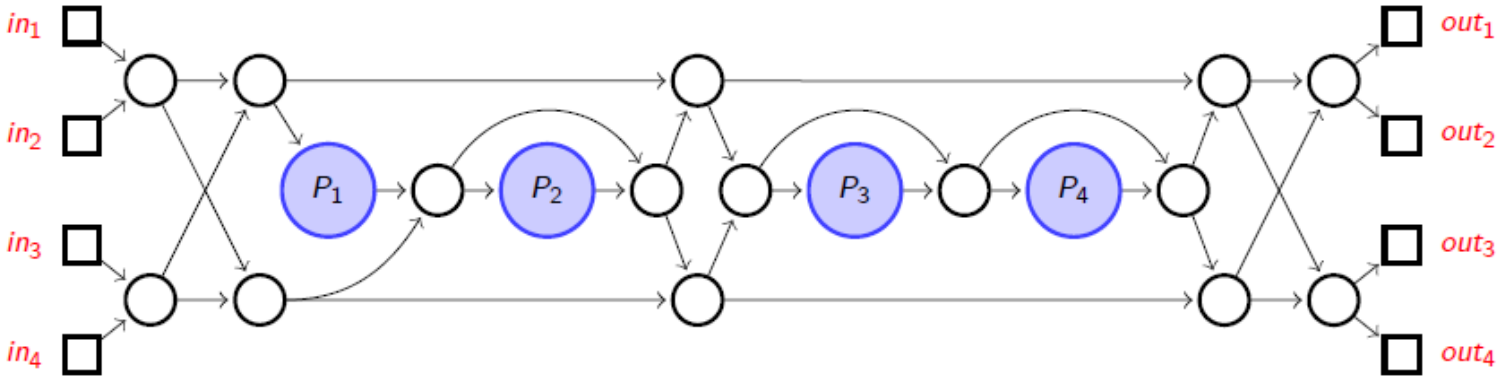
[**Valiant76**]: $\mathrm{EUG_1}(\lceil n/k \rceil - 1)$ + k-way supernode $\mathrm{SN(k)} \rightarrow \mathrm{EUG_1(n)}$, then we have $|\mathrm{EUG_1(n)}| = \mathrm{k} \cdot |\mathrm{EUG_1}(\lceil n/k \rceil - 1)| + \lceil n/k \rceil \cdot |\mathrm{SN\ (k)}|$



Valiant's 2-way and 4-way Construction



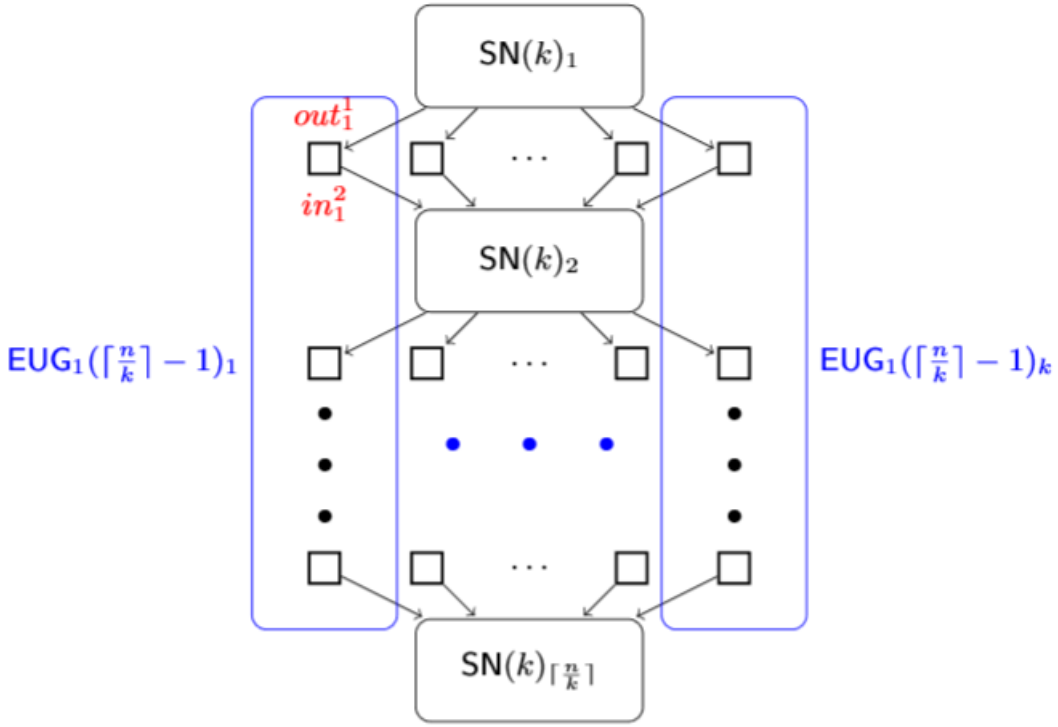
$$|SN(2)| = 5 \ , \ |\mathrm{EUG}_2(n)| = 5n \log n$$

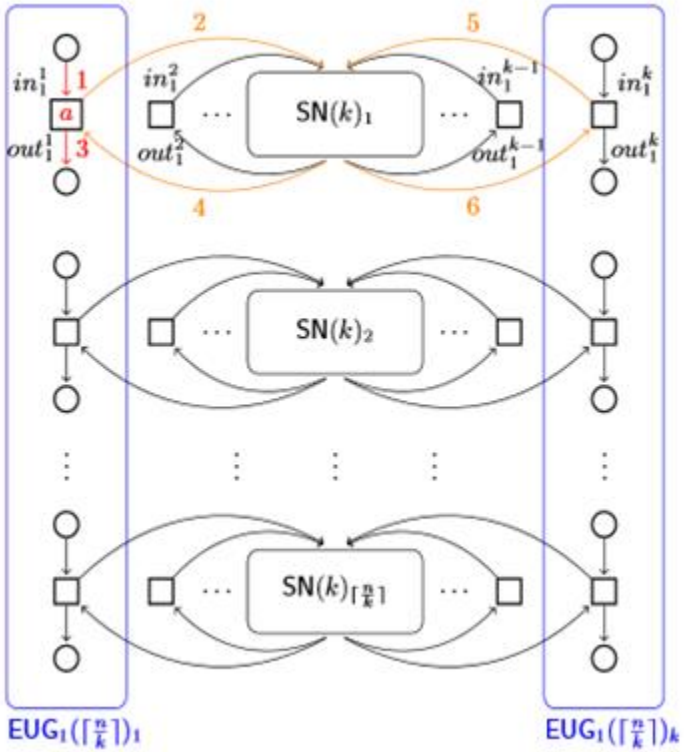


$$|SN(4)| = 19 \ , \ |\mathrm{EUG}_2(n)| = 4.75n \log n$$

Our Construction

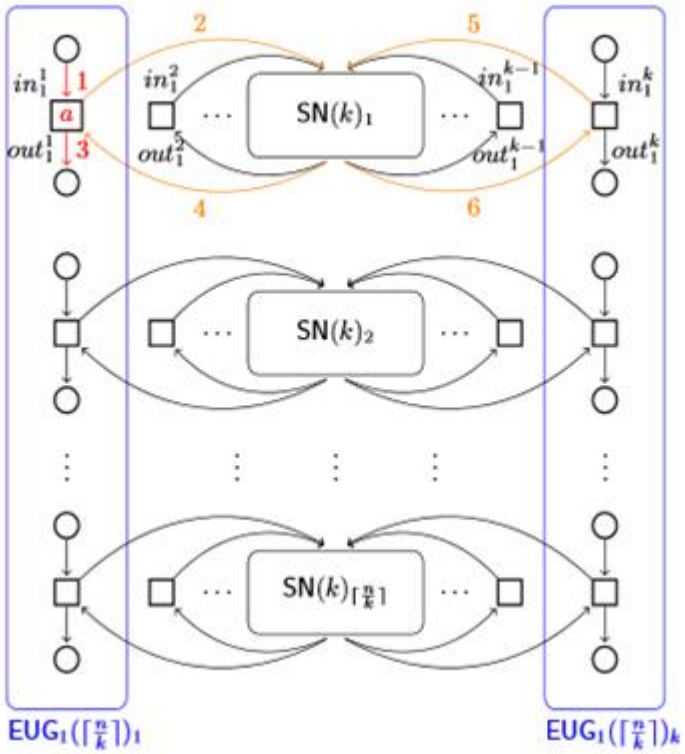
Valiant's framework vs. Our intermediate construction

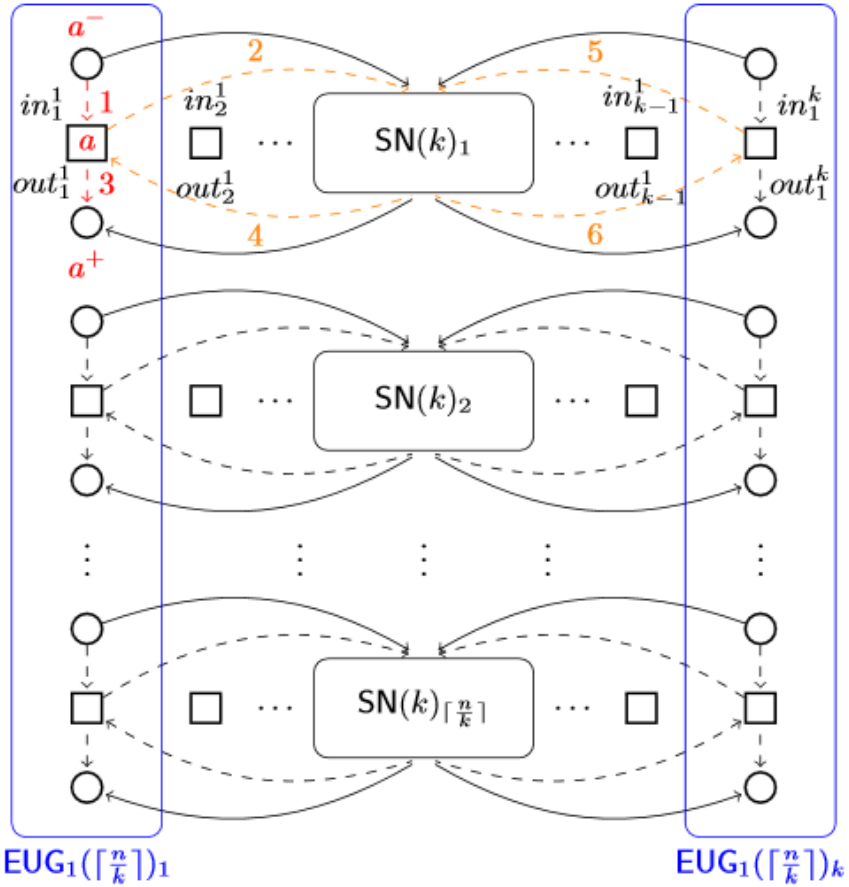




Our Construction

Our intermediate construction vs. Our end construction





Our End Construction: Size of Circuit

$$|\mathsf{EUG}_2(n)| = 2|\mathsf{EUG}_1(n)| - n$$

$$|\mathsf{EUG}_1(n)| = k \cdot |\mathsf{EUG}_1(\lceil \frac{n}{k} \rceil)| + \lceil \frac{n}{k} \rceil \cdot |\mathsf{SN}(k)| - n \ .$$

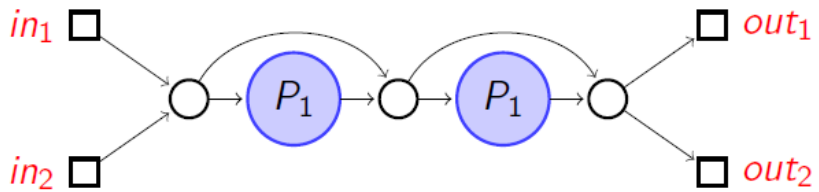
Theorem 4 (Universal circuits). *For any integer $k \geq 2$, there exists explicit k-way constructions of $\mathsf{EUG}_2(n)$ and UC_n with*

$$|\mathsf{EUG}_2(n)| = \frac{2(|\mathsf{SN}(k)| - k)}{k \log k} n \log n - O(n)$$

≥ 2.95

$$|\mathsf{UC}_n| \leq 4|\mathsf{EUG}_2(n)| + O(n) \ .$$

In particular, for $k = 2$ we have $|\mathsf{EUG}_2(n)| = 3n \log n - O(n)$.



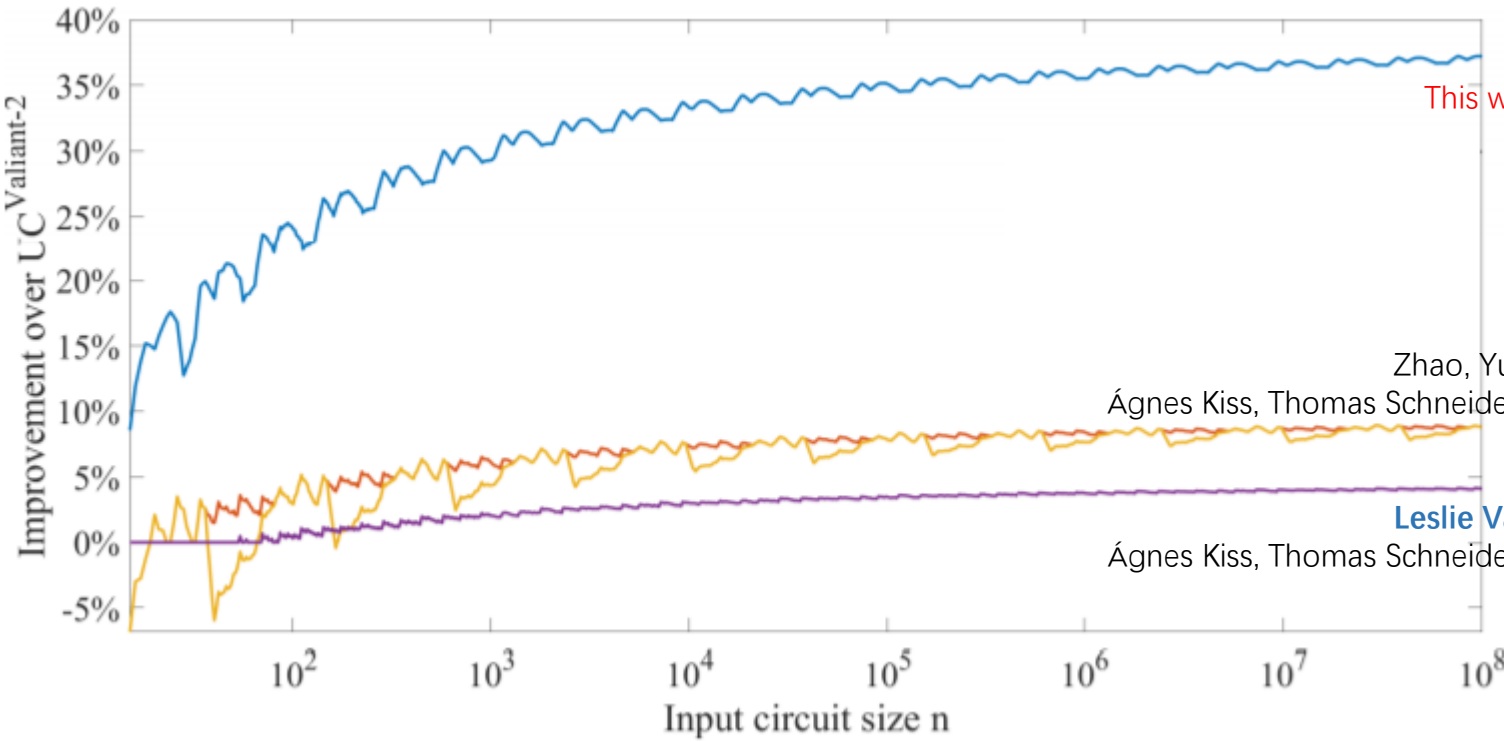
$|SN(2)| = 5$, $|\mathsf{EUG}_2(n)| = 3n \log n - O(n)$.

Comparison with Previous Works

Asymptotic size of $EUG_2(n)$:

Construction	Leslie Valiant STOC 1976	Günther, Kiss & Schnerider EUROCRYPT2016, ASIACRYPT 2017	Zhao Yu et al. ASIACRYPT 2019	Liu Yu et al. CRYPTO 2021
$\lvert EUG_2(n)\rvert$	$\sim 4.75n \cdot \log n$	$\sim 4.75n \cdot \log n$	$\sim 4.5n \cdot \log n$	$\sim 3n \cdot \log n$

Close to lower bound: $2.95n \cdot \log n$



This work

Zhao, Yu, et.al. **ASIACRYPT 2019**
Ágnes Kiss, Thomas Schneider et.al. **Journal of Cryptology 2020**

Leslie Valiant **STOC 1976**
Ágnes Kiss, Thomas Schneider et.al **EUROCRYPT 2016**
ASIACRYPT 2017

Related Works

- Leslie Valiant, *Universal Circuit*, **STOC 1976**
- Helger Lipmaa, Payman Mohassel, Saeed Sadeghian. *Valiant's Universal Circuit: Improvements, Implementation, and Applications*, **ePrint 2016/017**
- Ágnes Kiss, Thomas Schneider. *Valiant's Universal Circuit is Practical,* **EUROCRYPT 2016**
- Daniel Günther, Ágnes Kiss, Thomas Schneider. *More Efficient Universal Circuit Constructions*, **ASIACRYPT 2017**
- Shuoyao Zhao, Yu Yu, Jiang Zhang, **Hanlin Liu**. *Valiant's Universal Circuits Revisited: an Overall Improvement and a Lower Bound*, **ASIACRYPT 2019**
- Masaud Y. Alhassan, Daniel Günther, Ágnes Kiss, Thomas Schneider. *Efficient and Scalable Universal Circuits*, **Journal of Cryptology 2020**

Thanks for Listening!