Pung

Unobservable communication over fully untrusted infrastructure

Sebastian Angel (UT Austin) & Srinath Setty (Microsoft Research) at OSDI '16

Sze Chuen Tan

“Metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.”

Stewart Baker, Former NSA General Counsel

“Metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.”

Stewart Baker, Former NSA General Counsel

“We kill people based on metadata.”

General Michael Hayden, Former NSA and CIA Director

In response to Baker

https://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/


Alice


Alice
Wedding Planner
Obstetrician
Insurance Agent

Alice

3,464,282 views | Feb 16, 2012, 11:02am

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill Forbes Staff

Welcome to The Not-So Private Parts where technology & privacy collide

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT -0.14%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Target has got you in its aim

Wedding Planner

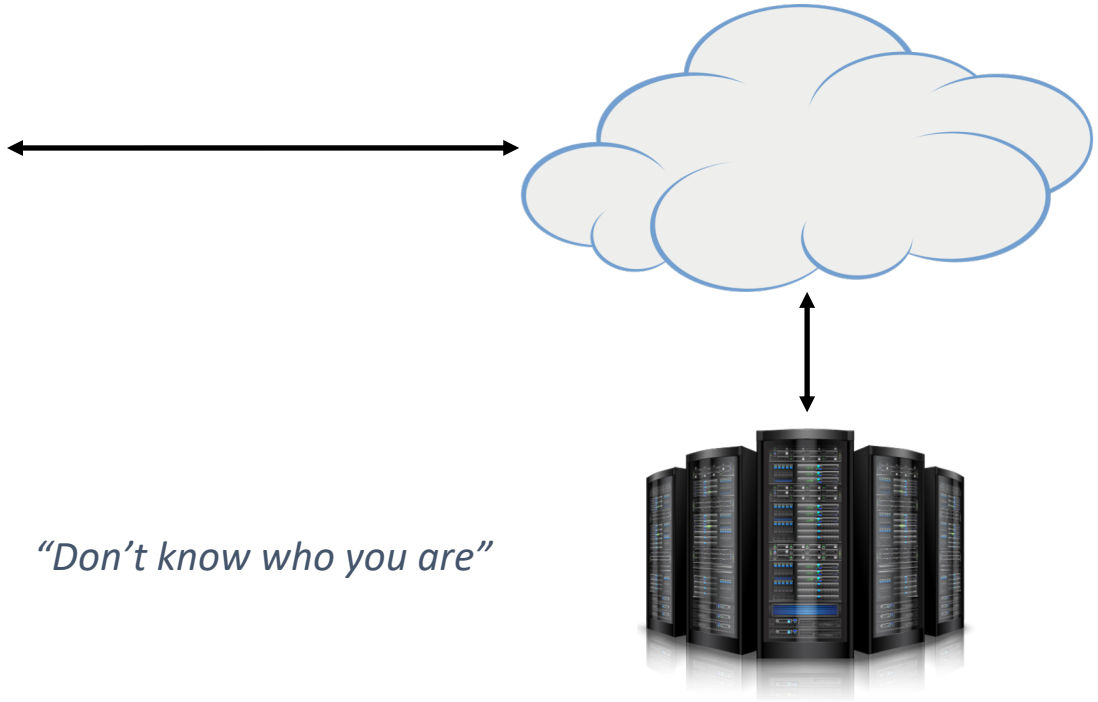
Obstetrician

Insurance Agent

Mix Network (“mixnet”)
Atom , Loopix , Stadium, Vuvuzela, Pynchon*, Riffle*

Dining Cryptographers Network (“DC-net”)
Dissent

Private Information Retrieval (“PIR”)
DP5, e-PIR, Popcorn, Pung, Riposte, Talek, Pynchon*, Riffle*

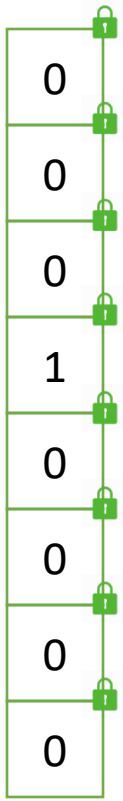


“Don’t know who you are”

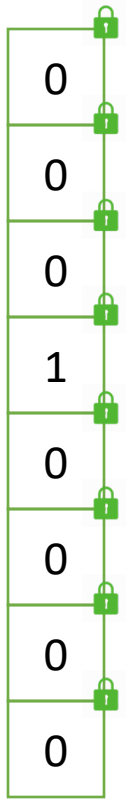
“Don’t know what you’ve requested”

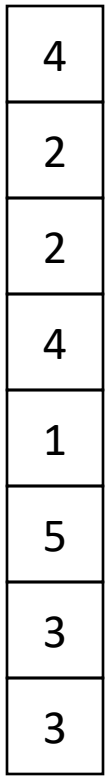
0
0
0
1
0
0
0
0

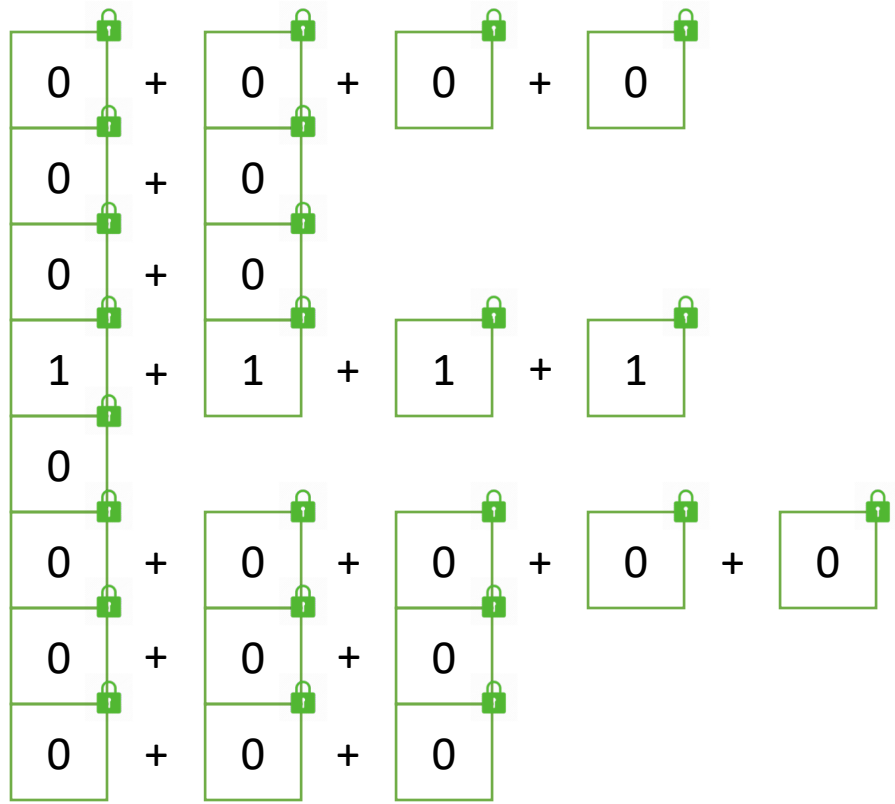
4
2
2
4
1
5
3
3



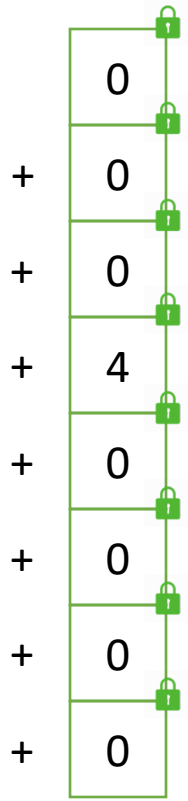
4
2
2
4
1
5
3
3


0
0
0
1
0
0
0
0


4
2
2
4
1
5
3
3



4
2
2
4
1
5
3
3



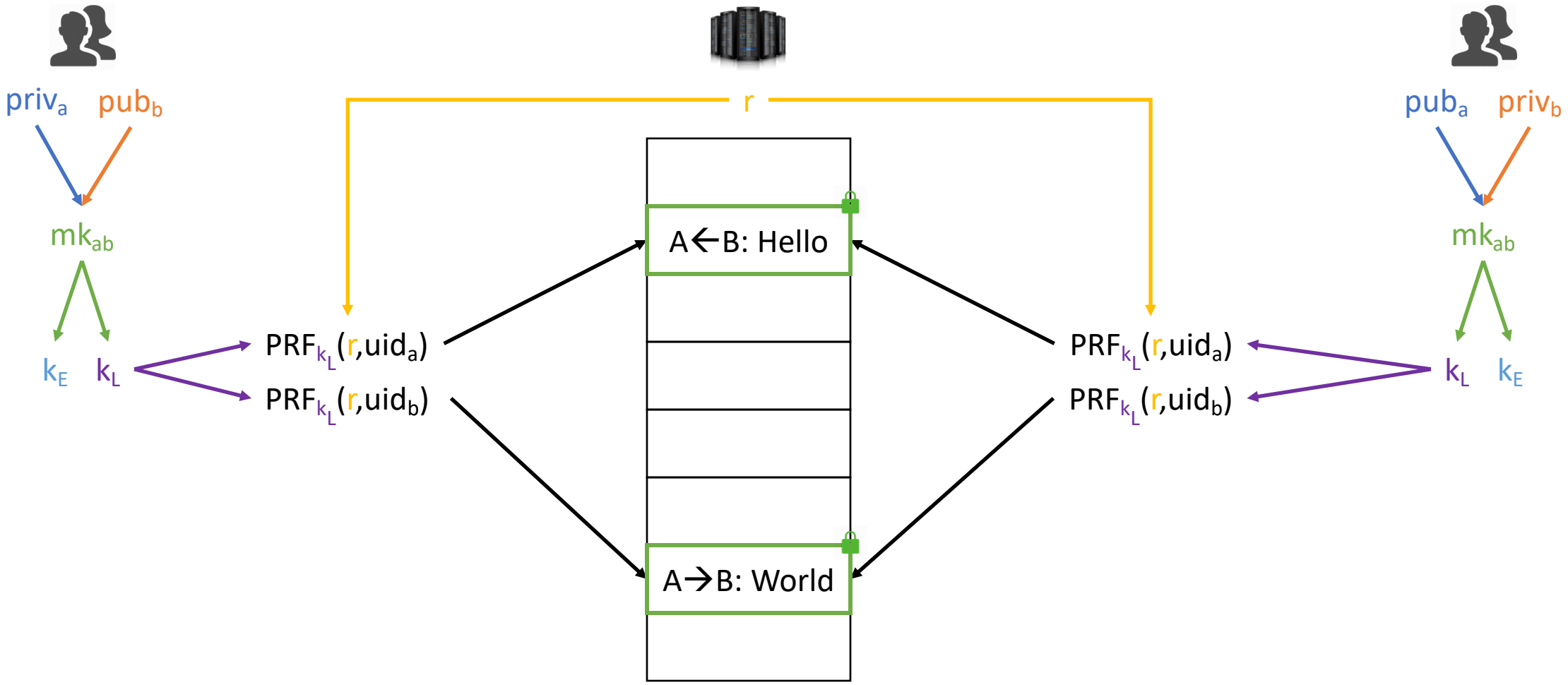
4
2
2
4
1
5
3
3

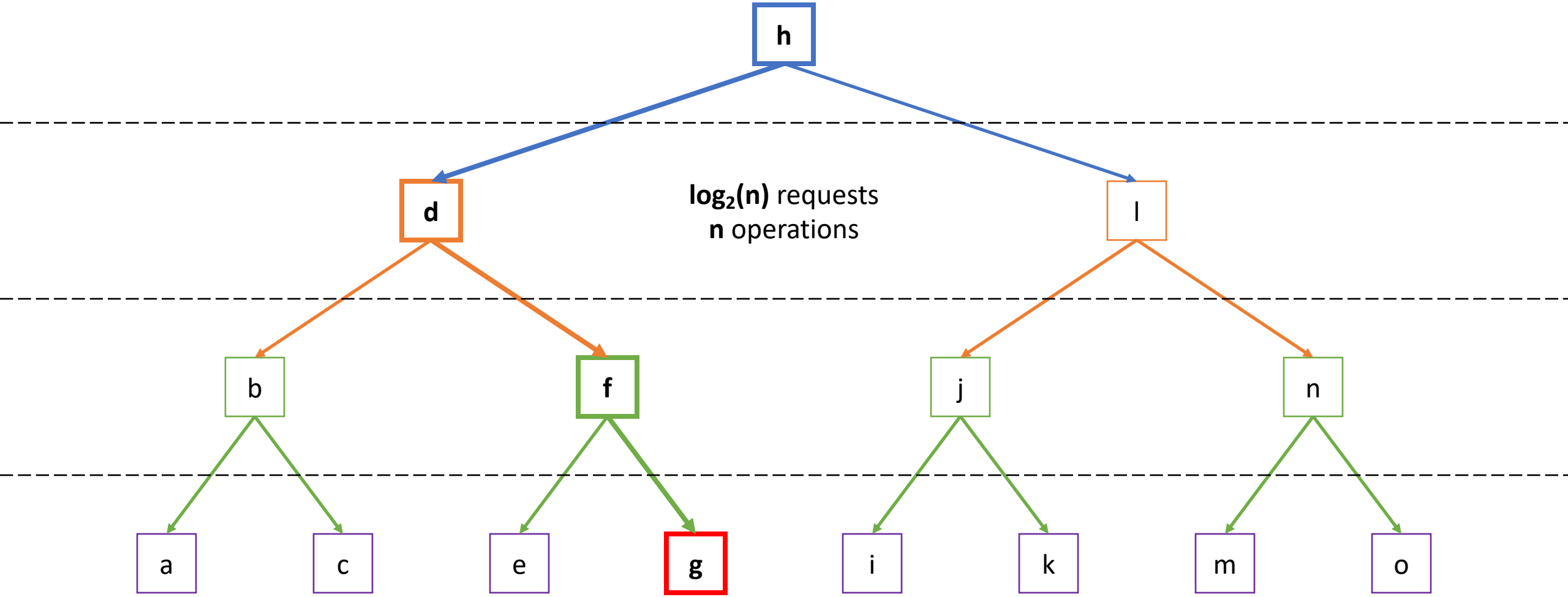
4
2
2
4
1
5
3
3

4
2
2
4
1
5
3
3

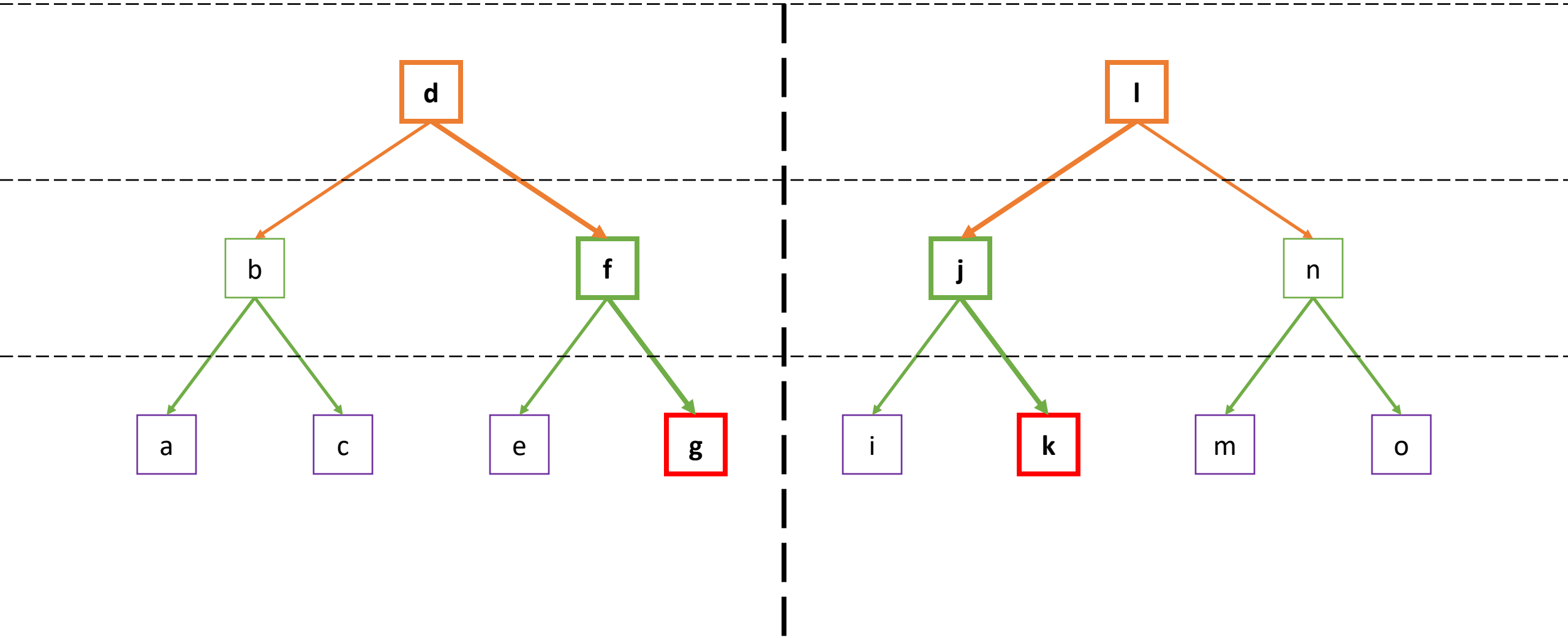
4

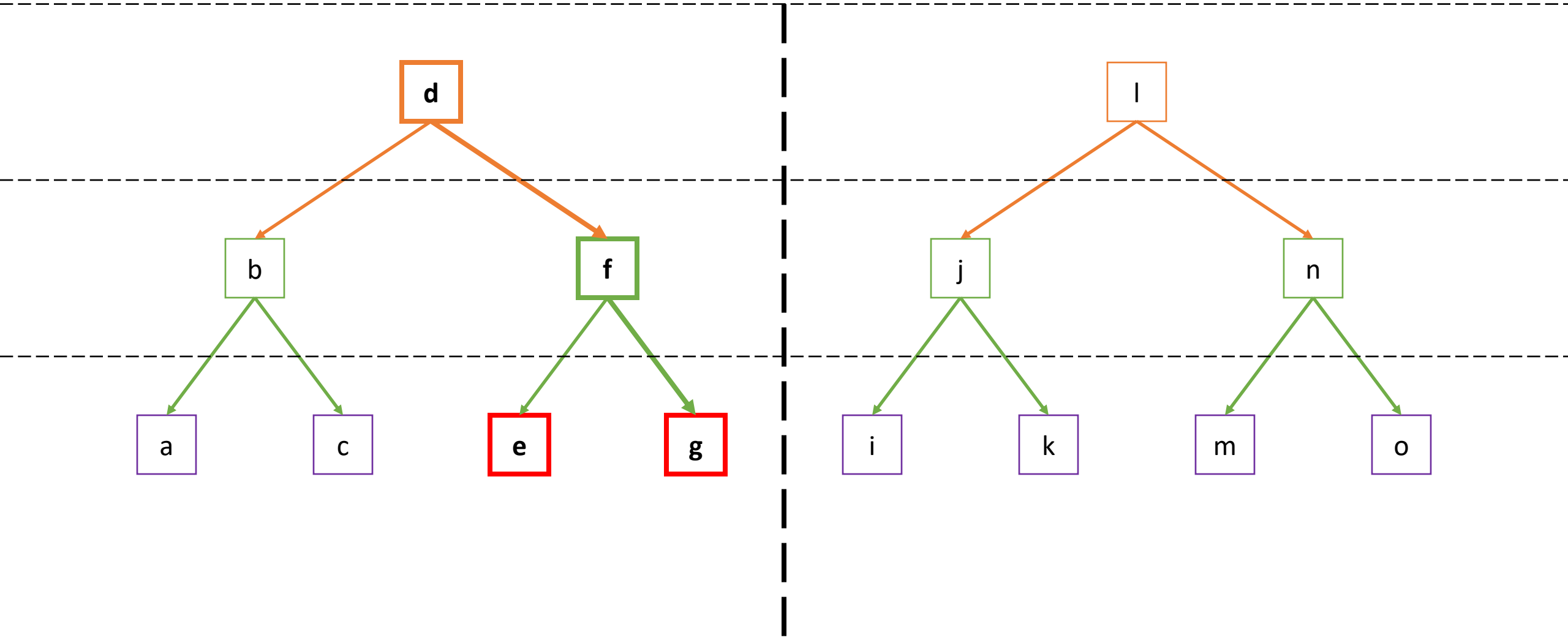
4
2
2
4
1
5
3
3

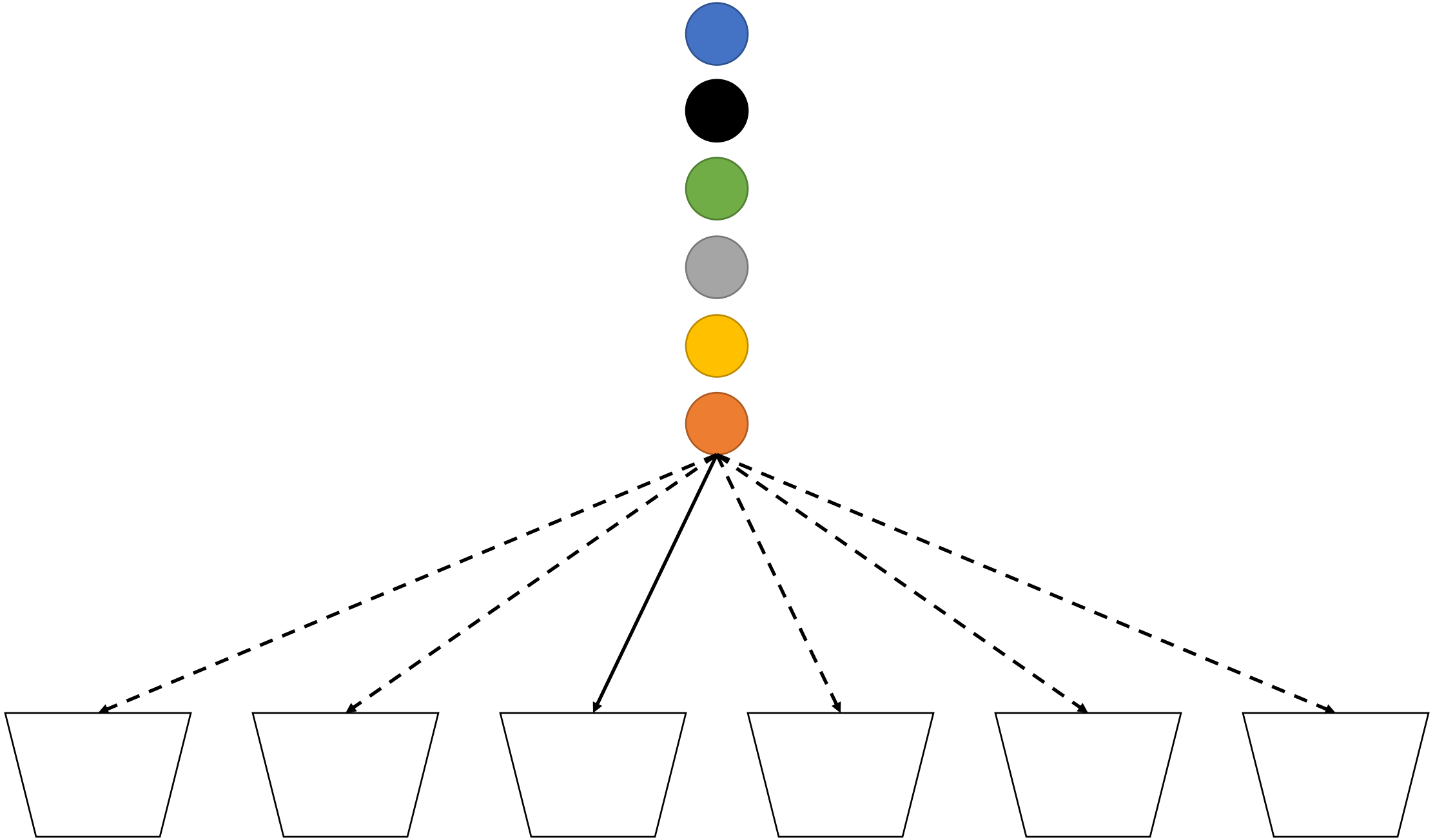

priv_a
pub_b
mk_ab
k_E
k_L
r
PRF_kL(r,uid_a)
PRF_kL(r,uid_b)
A←B: Hello
A→B: World
PRF_kL(r,uid_a)
PRF_kL(r,uid_b)
pub_a
priv_b
mk_ab
k_L
k_E


h
d
l
b
f
j
n
a
c
e
g
i
k
m
o
log2(n) requests
n operations

$\log_2(n/k)$ requests
n/k operations

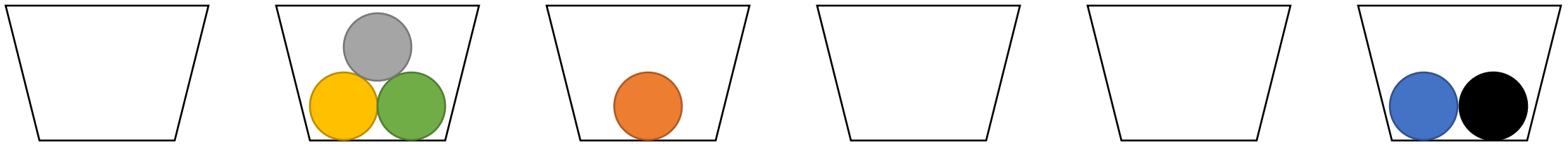


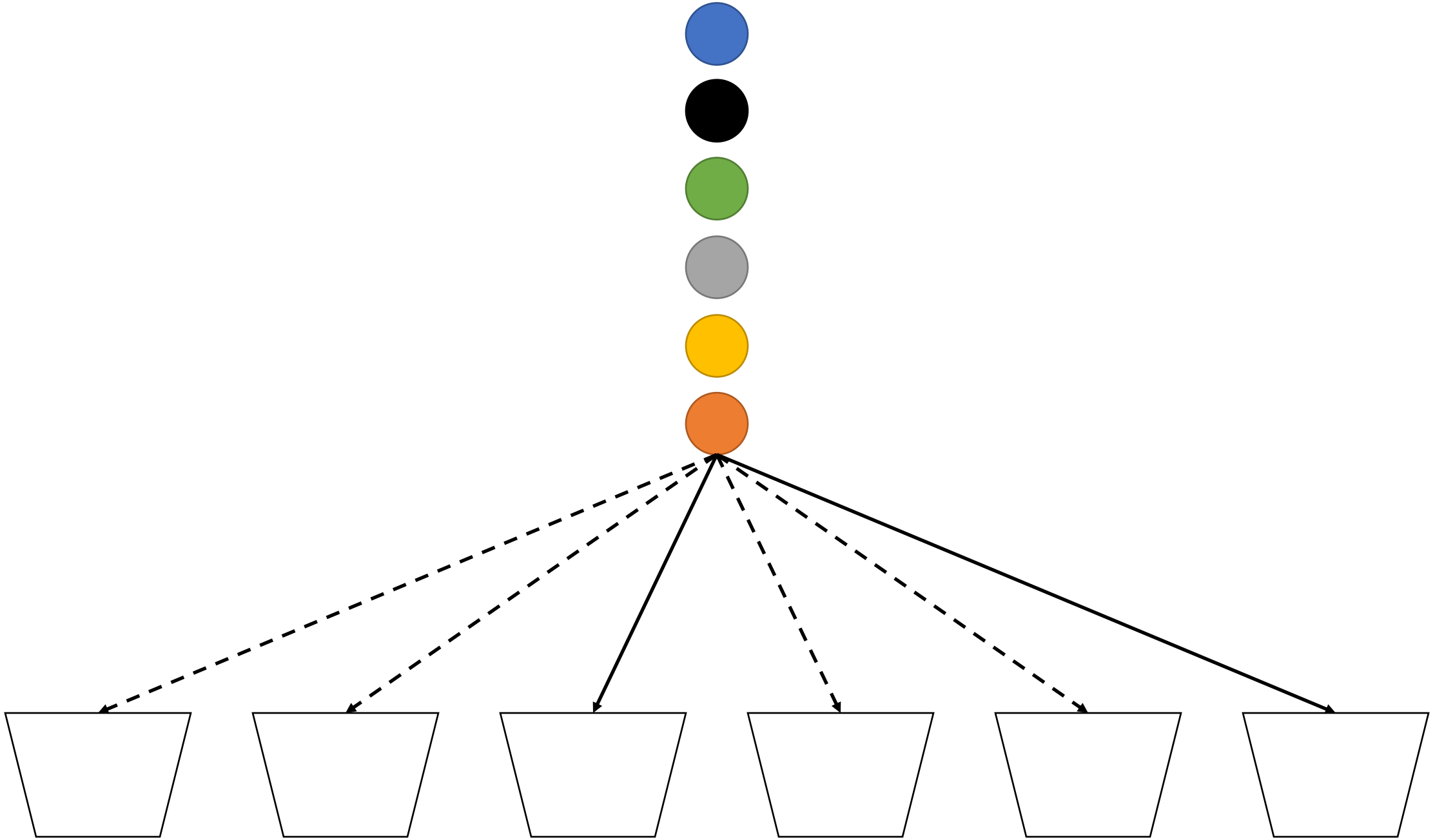

d
b
f
a
c
e
g
l
j
n
i
k
m
o

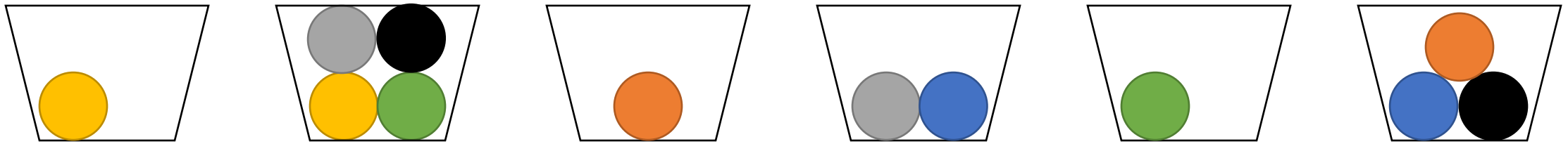


$$Pr\left(\rho \geq \frac{3\ln(k)}{\ln(\ln(k))}\right) \leq \frac{1}{k}$$

```
8.16 for k= 16      9.22 for k=128
8.37 for k= 32      9.71 for k=256
8.75 for k= 64      10.2 for k=512
```

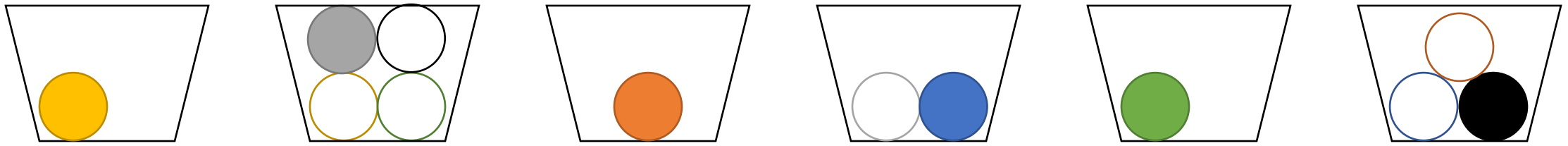




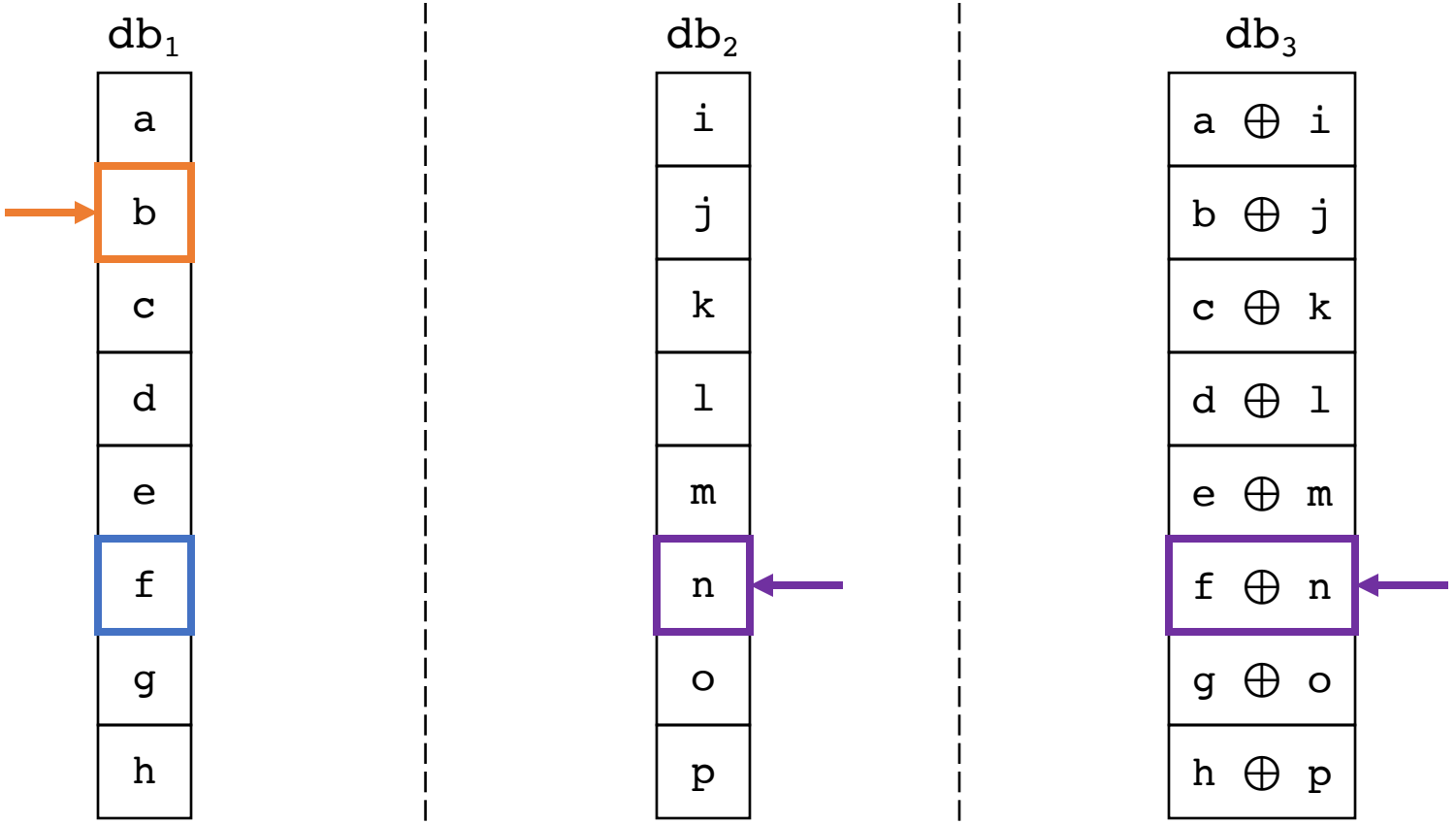


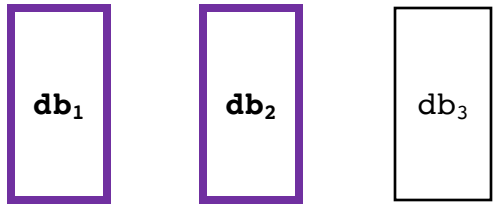
$$Pr\left(\rho \geq \frac{\ln(\ln(k))}{\ln(2)}\right) \leq o(1)$$

```
1.47 for k= 16      2.28 for k=128
1.79 for k= 32      2.47 for k=256
2.06 for k= 64      2.64 for k=512
```



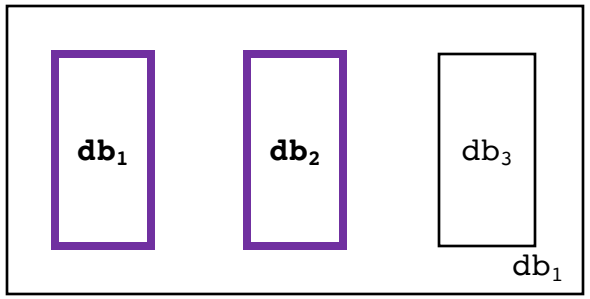
(n,3/2n,2,3)

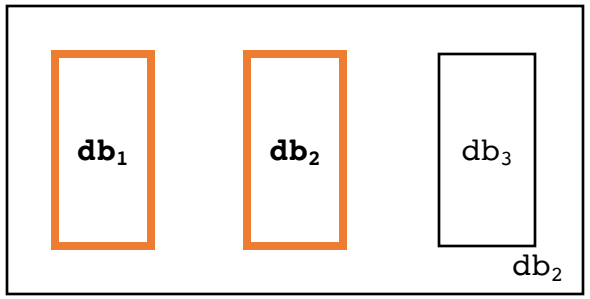


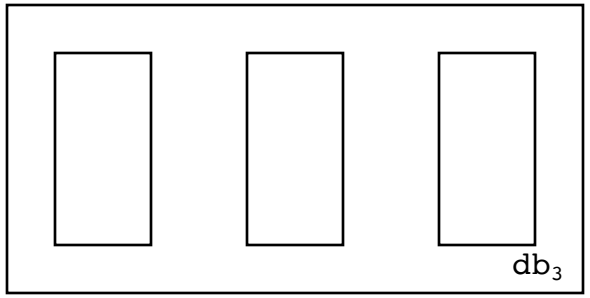


3/2 ≈ 1.5 req, (3/2n)/2 ≈ .75n ops

(n, 3/2n,2, 3)

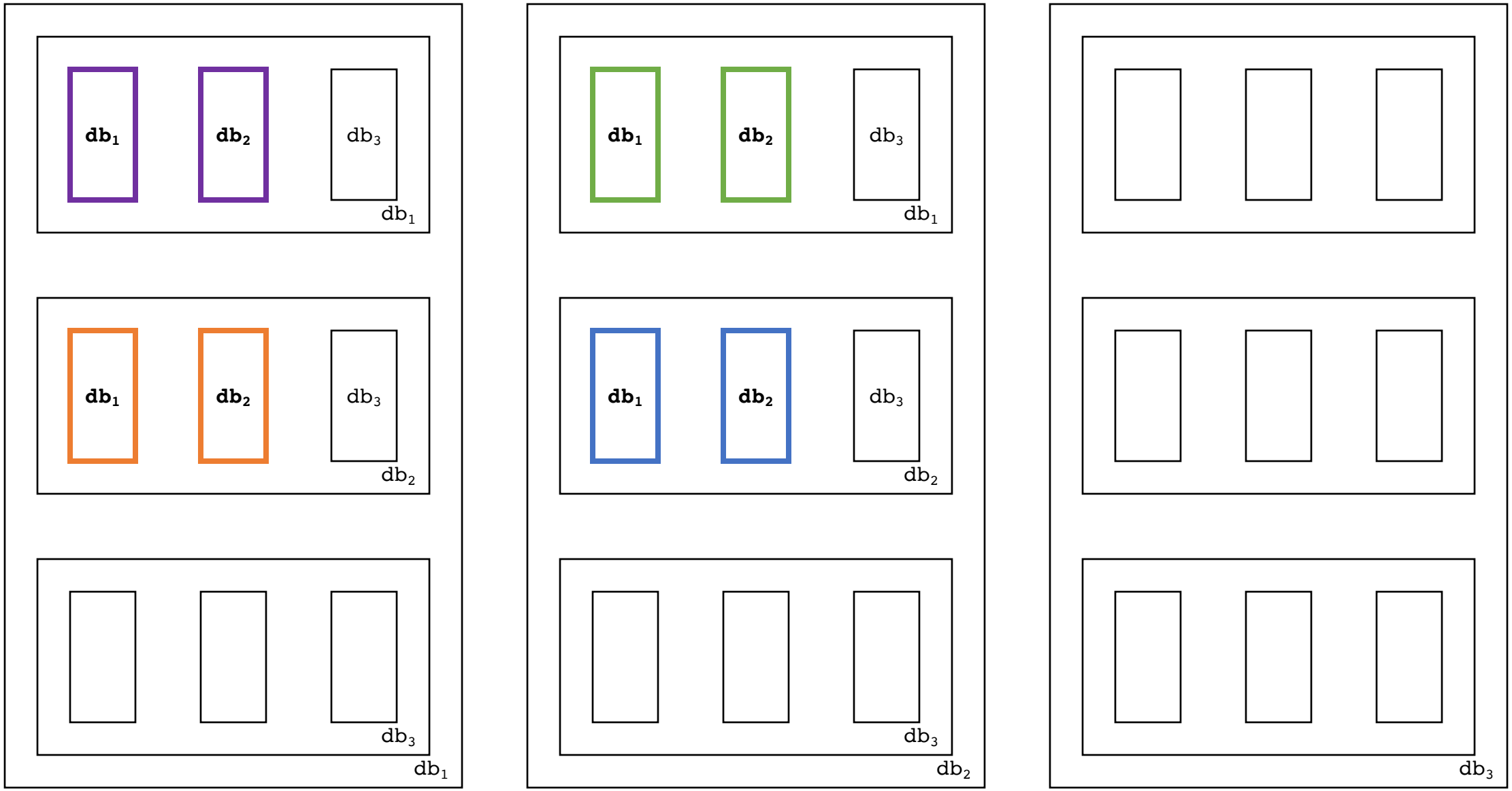






9/4 ≈ 2.3 req, (9/4n)/4 ≈ .56n ops

(n, 9/4n,4, 9)



27/8 ≈ 3.4 req, (27/8n)/8 ≈ .42n ops

(n,27/8n,8,27)

n=1000000

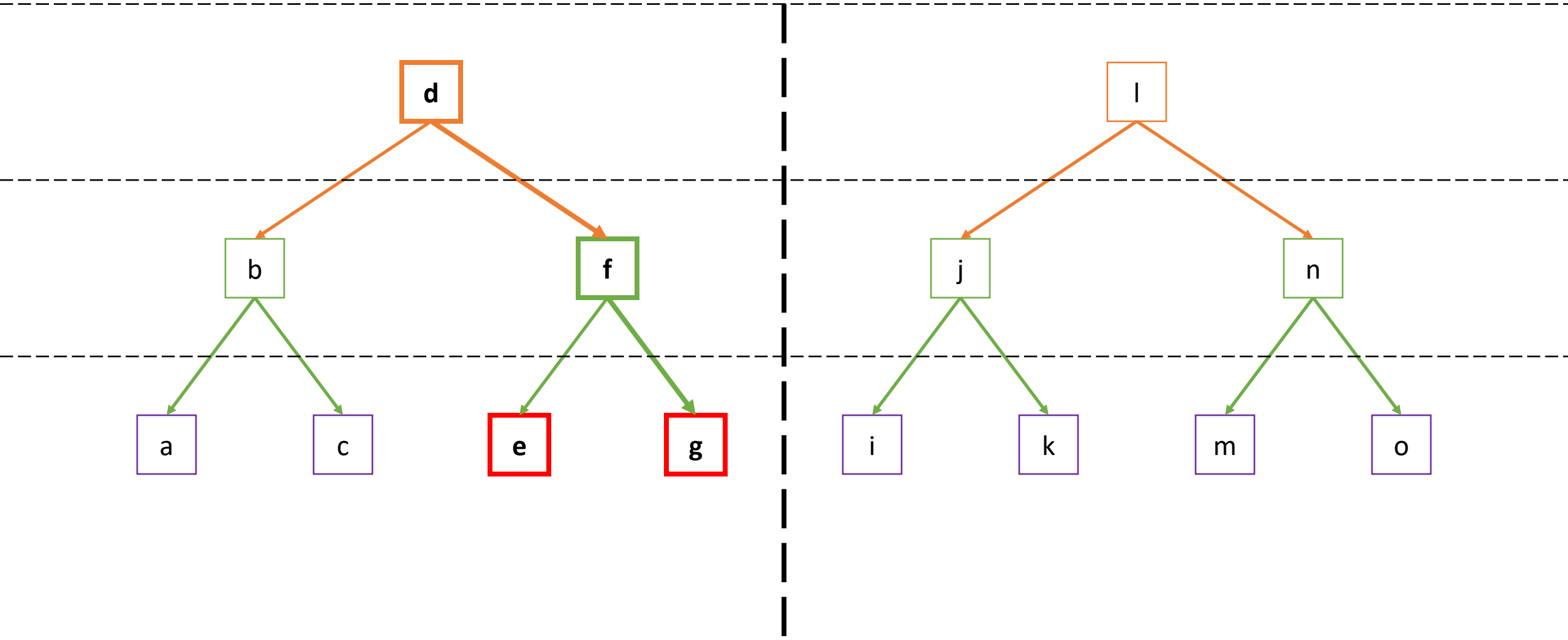
	BST Power of 2		Batch Coding	
	req $\frac{3^{log_2(k)}}{k}$	ops $\frac{3^{log_2(k)}}{k^2}n$	req $\frac{\ln(\ln(k))}{\ln(2)}log_2(\frac{n}{k})$	ops $\frac{\ln(\ln(k))}{\ln(2)}\frac{n}{k}$
k= 2	1.50	750k	19	500k
k= 4	2.25	562k	18	250k
k= 8	3.38	422k	34	250k
k= 16	5.06	316k	32	125k
k= 32	7.59	237k	30	63k

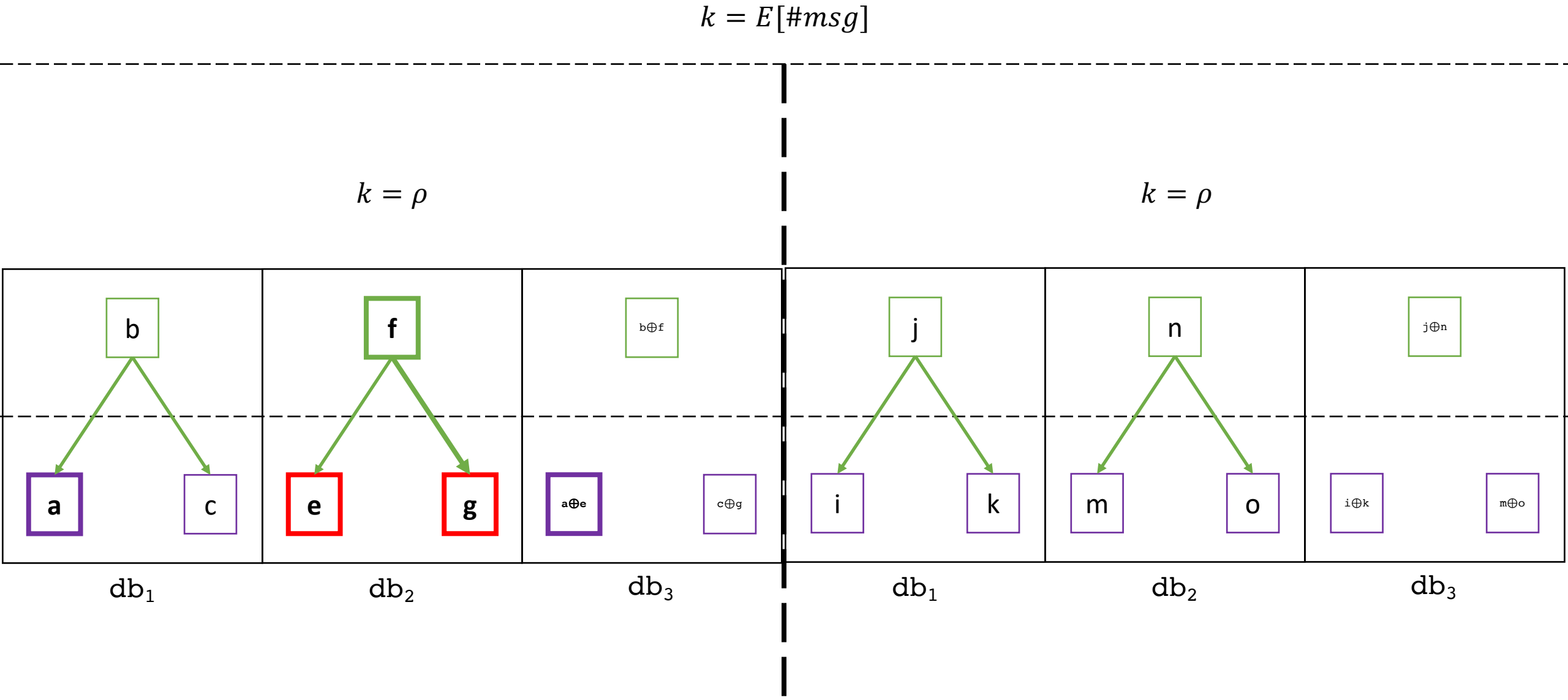
	BST Power of 2		Batch Coding	
	req $\frac{3^{log_2(k)}}{k}$	ops $\frac{3^{log_2(k)}}{k^2}n$	req $\frac{\ln(\ln(k))}{\ln(2)}log_2(\frac{n}{k})$	ops $\frac{\ln(\ln(k))}{\ln(2)}\frac{n}{k}$
k= 64	11.4	178k	42	46k
k= 128	17.1	133k	39	23k
k= 256	25.6	100k	36	11k
k= 512	38.4	75k	33	5.9k
k=1024	57.7	56k	30	2.9k

n=1000

	BST Power of 2		Batch Coding	
	req $\frac{3^{log_2(k)}}{k}$	ops $\frac{3^{log_2(k)}}{k^2}n$	req $\frac{\ln(\ln(k))}{\ln(2)}log_2(\frac{n}{k})$	ops $\frac{\ln(\ln(k))}{\ln(2)}\frac{n}{k}$
k= 2	1.50	750	9	500
k= 4	2.25	562	8	250
k= 8	3.38	422	14	250
k= 16	5.06	316	12	125
k= 32	7.59	237	10	63

	BST Power of 2		Batch Coding	
	req $\frac{3^{log_2(k)}}{k}$	ops $\frac{3^{log_2(k)}}{k^2}n$	req $\frac{\ln(\ln(k))}{\ln(2)}log_2(\frac{n}{k})$	ops $\frac{\ln(\ln(k))}{\ln(2)}\frac{n}{k}$
k= 64	11.4	178	12	46
k= 128	17.1	133	9	23
k= 256	25.6	100	6	11
k= 512	38.4	75	3	5.9
k=1024	57.7	56	3	2.9


d
b
f
a
c
e
g
l
j
n
i
k
m
o


$k = E[\#msg]$
$k = \rho$
$k = \rho$
b
f
b⊕f
j
n
j⊕n
a
c
e
g
a⊕e
c⊕g
i
k
m
o
i⊕k
m⊕o
db_1
db_2
db_3
db_1
db_2
db_3

Comments

Assumption that a large number of messages are to be retrieved every epoch for amortization to work

High network costs

Scalability

Centralized point of failure

Participation even when client has no message to send/receive

Key distribution problem

Similarity to ORAM techniques