black hat USA 2019

AUGUST 3-8, 2019

MANDALAY BAY / LAS VEGAS

#BHUSA @BLACK HAT EVENTS

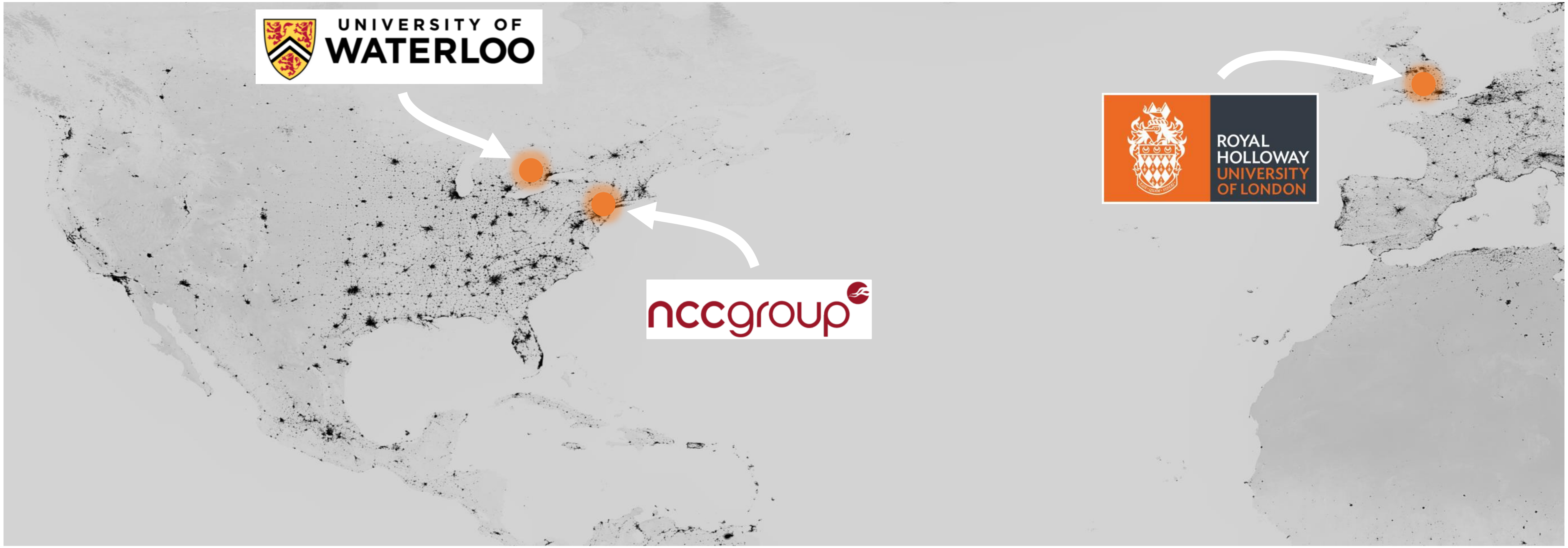
BREAKING ENCRYPTED DATABASES: GENERIC ATTACKS ON RANGE QUERIES

Marie-Sarah Lacharité

Royal Holloway, University of London
and NCC Group

black hat USA 2019
AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS

About Me


UNIVERSITY OF WATERLOO
nccgroup
ROYAL HOLLOWAY UNIVERSITY OF LONDON

Motivation: Data Breaches

Entity	Type	Number of Records
First American	Finance	885,000,000
facebook	Social network apps	540,000,000
truecaller	Telephone directory	300,000,000
Capital One	Finance	106,000,000
Quest Diagnostics™	Clinical laboratory	11,900,000
Desjardins	Finance	2,900,000

';--have i been pwned?

Motivation: Data Breaches

Healthcare IT News

Walgreens company announces data breach

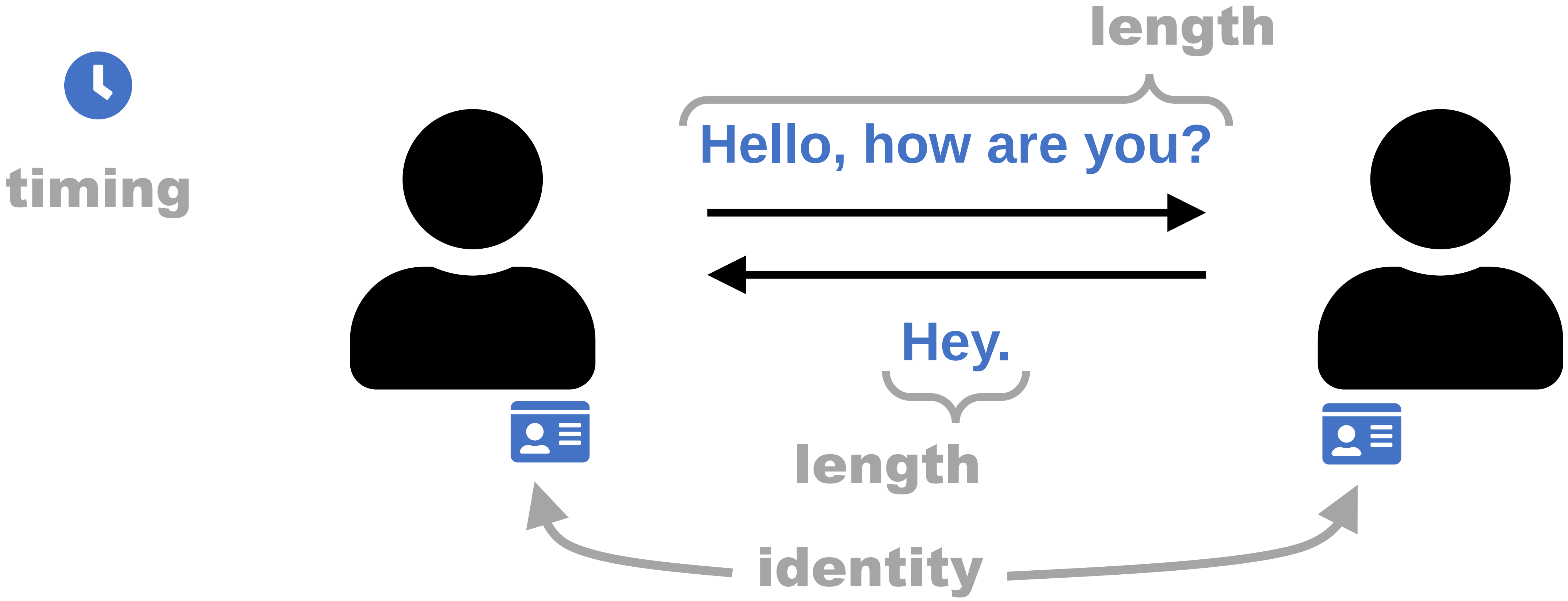
According to the letter, an unknown person or persons broke into Crescent's billing center and stole the hardware, which may have contained patient names, addresses, phone numbers, Social Security numbers, health insurance data, dates of birth and clinical diagnoses. The group notified authorities three days later.

WSJ CYBERSECURITY

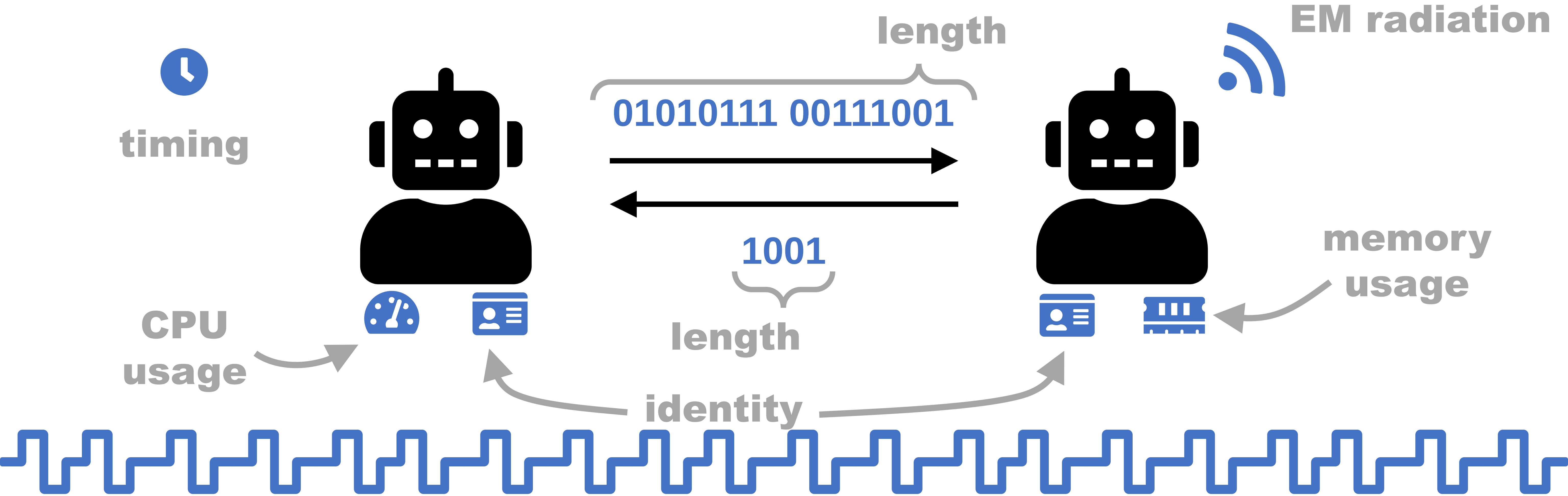
Capital One Breach Highlights Shortfalls of Encryption

Capital One said in a statement this week that it uses encryption "as a standard," but the method used by the hacker "enabled the decrypting of data." The bank didn't respond to questions about its encryption practices.

Side Channel Attacks



Side Channel Attacks



Side Channel Attacks

- SSH keystroke recovery from **timing** information

  [Song et al., USENIX 2001]

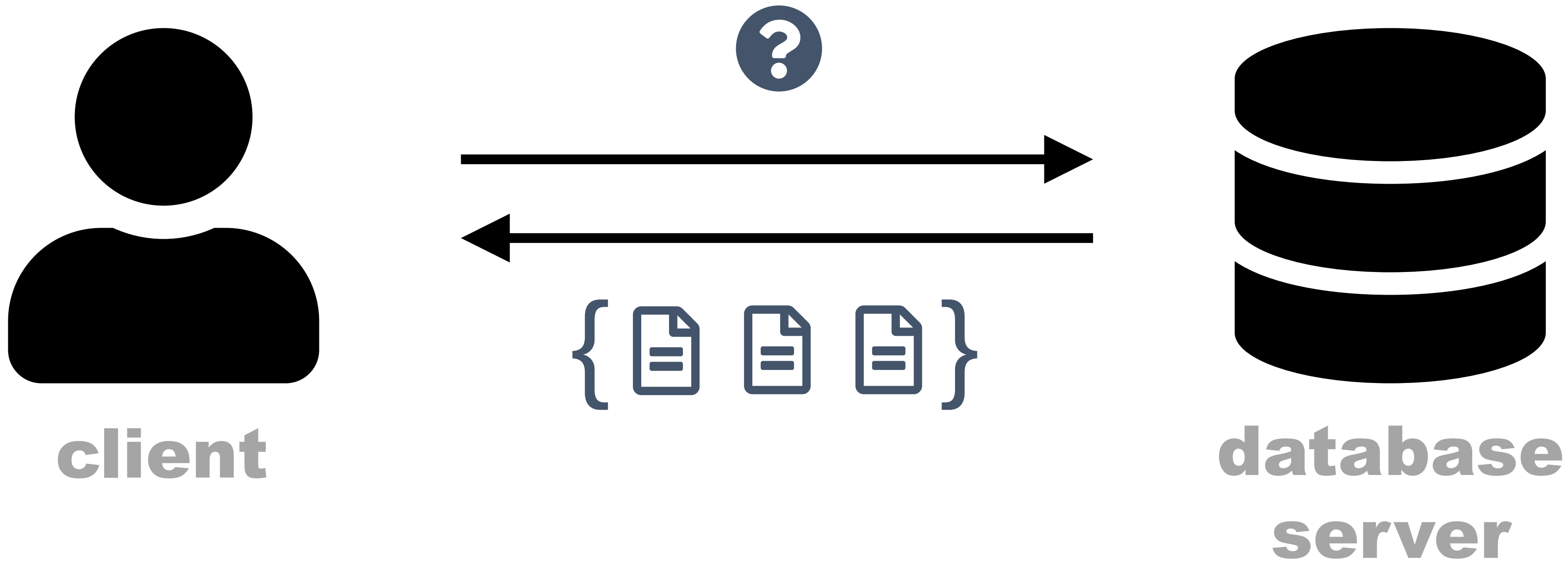
- Video stream identification from **traffic burst** analysis

  [Schuster et al., USENIX 2017]

- Message decryption from **padding validity** checks

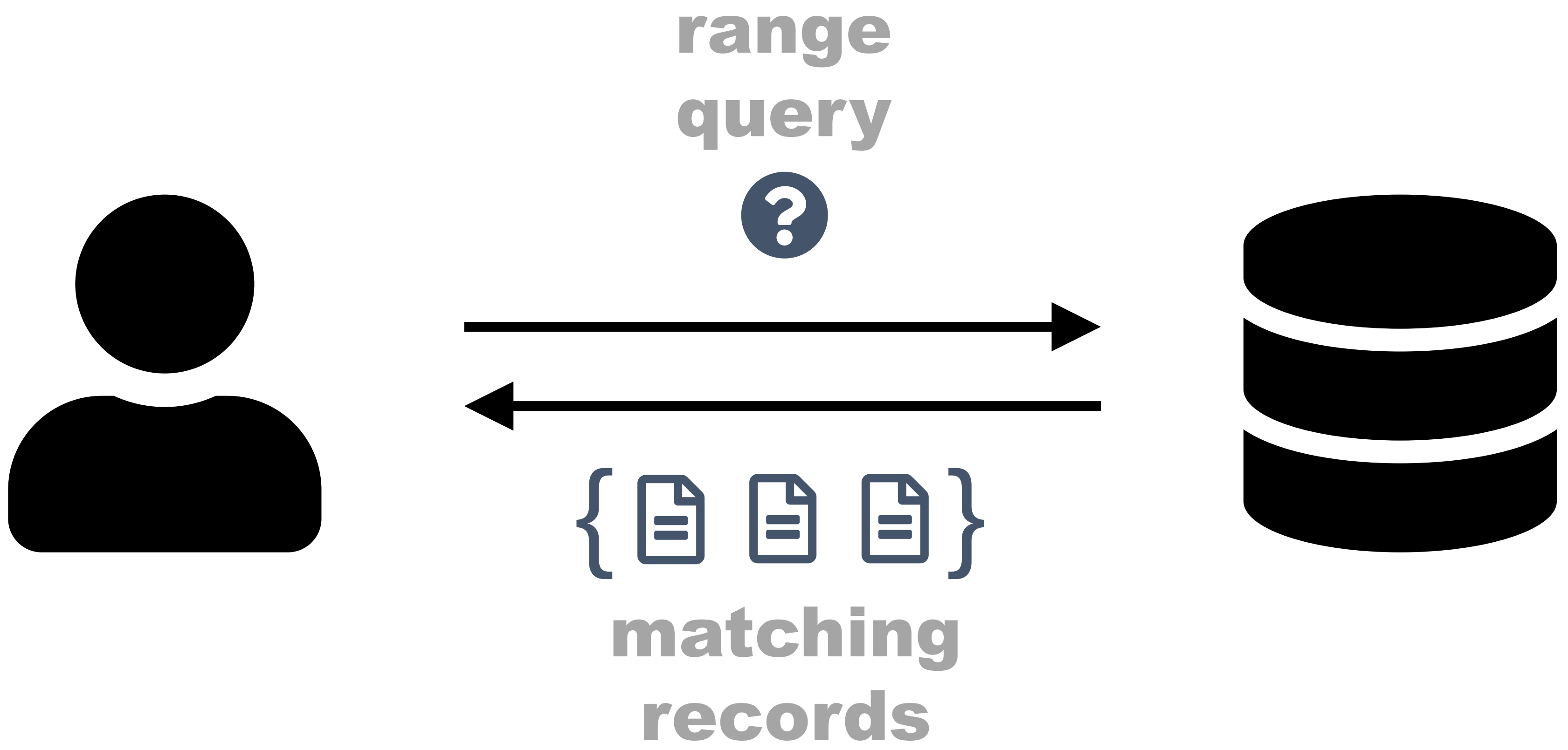
  [Bleichenbacher, CRYPTO 1998]

Encrypted Database Attacks



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypted Database Attacks

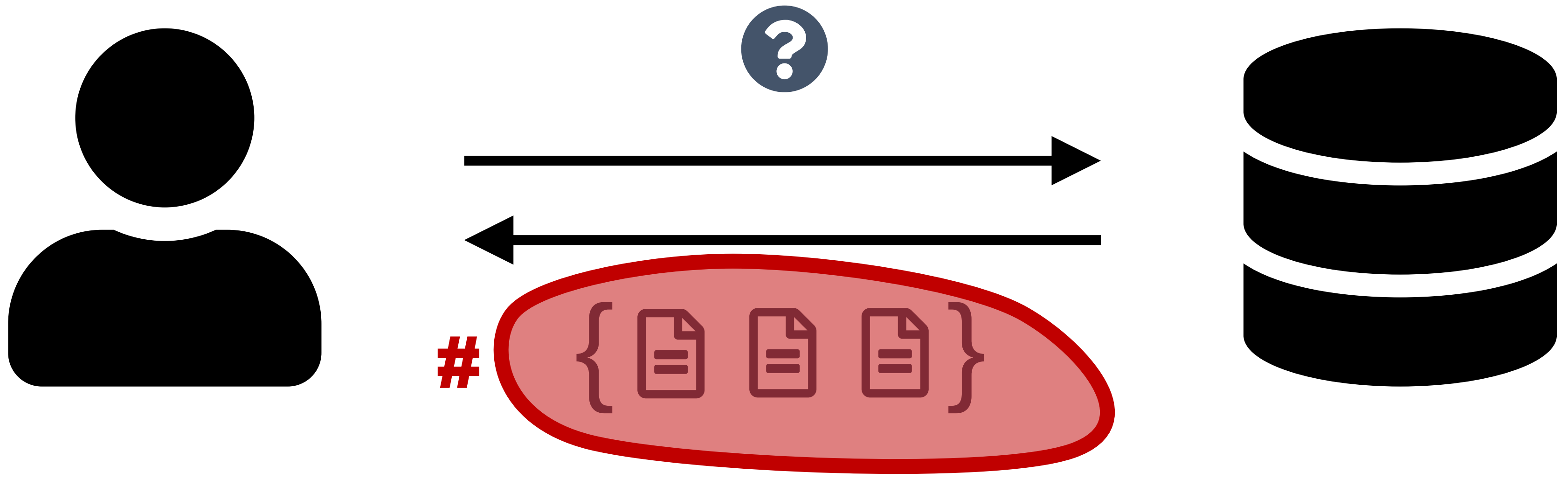


	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypted Database Attacks

access pattern leakage
(*which* records)

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…



volume leakage
(*how many* records)

Encrypted Database Attacks

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Outline

1. Existing approaches to securing a database
   - Securing data in transit, at rest, and in use

2. How to exploit leakage to break database encryption
   - Exploiting access pattern leakage and volume leakage

3. Security recommendations
   - Types of leakage, leaky operations, trade-offs

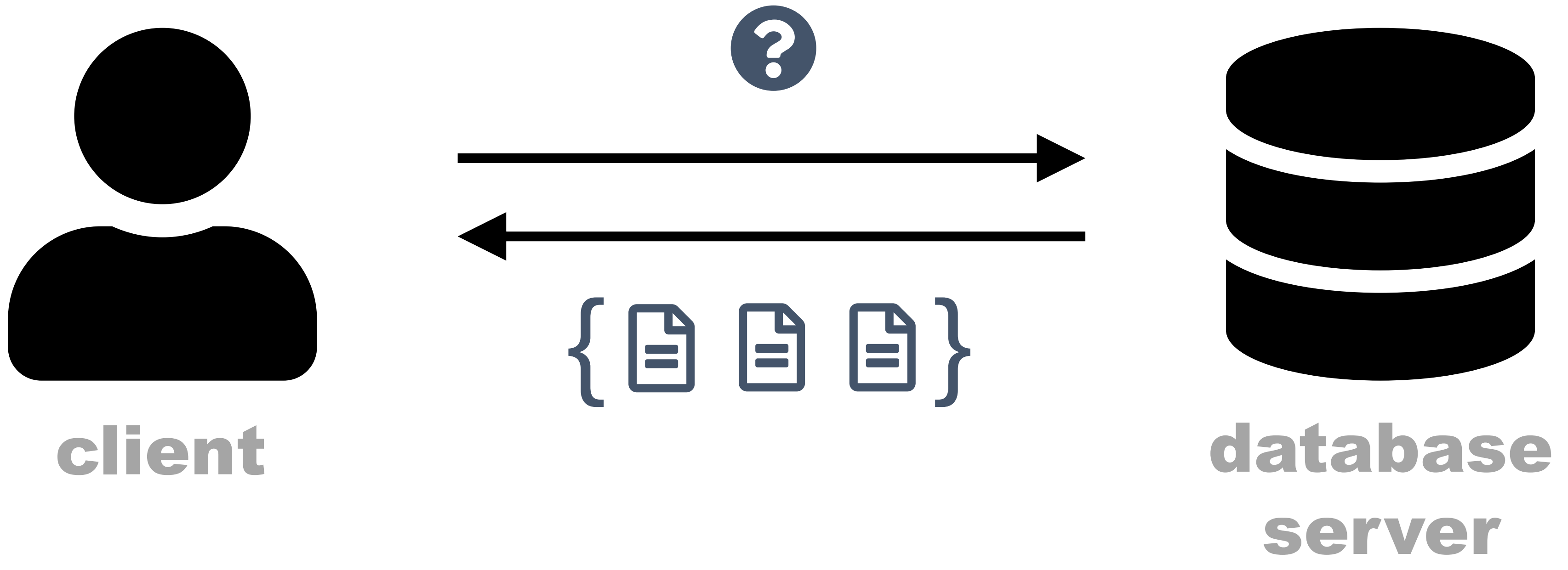
Outline

1. Existing approaches to securing a database
    - Securing data in transit, at rest, and in use

2. How to exploit leakage to break database encryption
    - Exploiting access pattern leakage and volume leakage

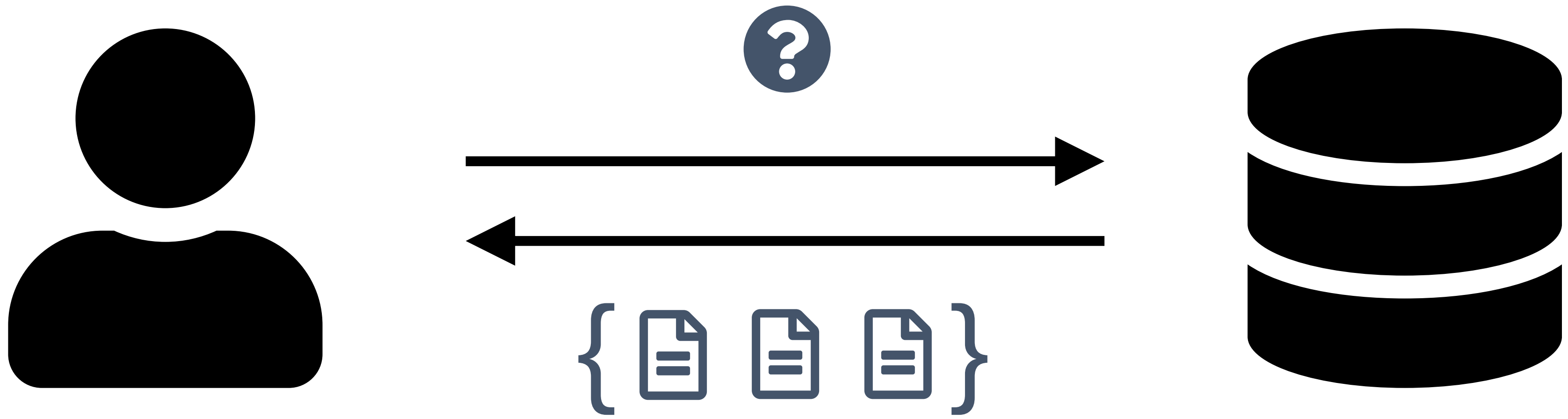
3. Security recommendations
    - Types of leakage, leaky operations, trade-offs

Model



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

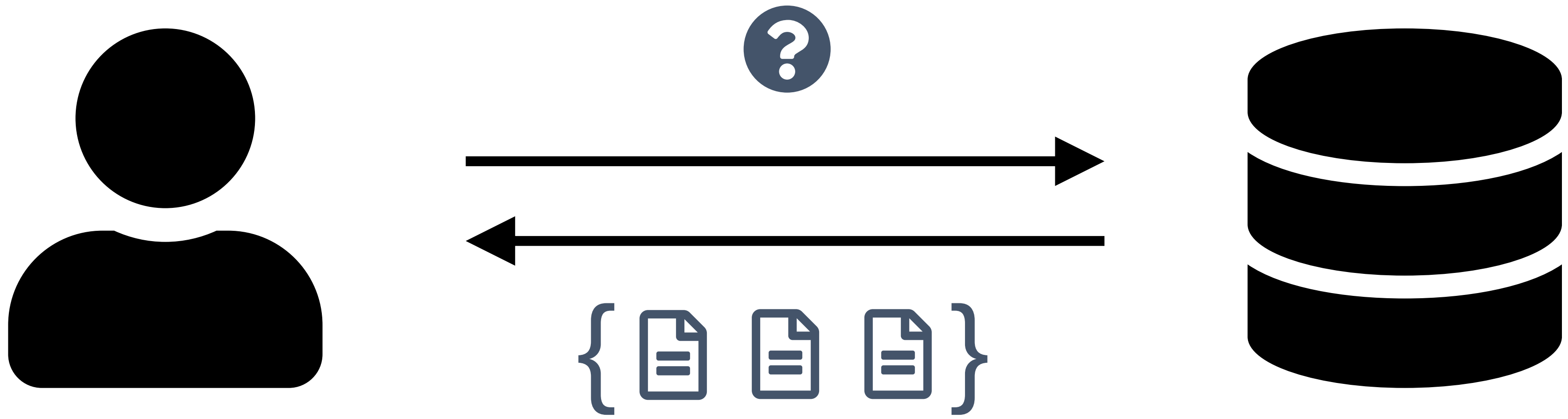
Model



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

database table

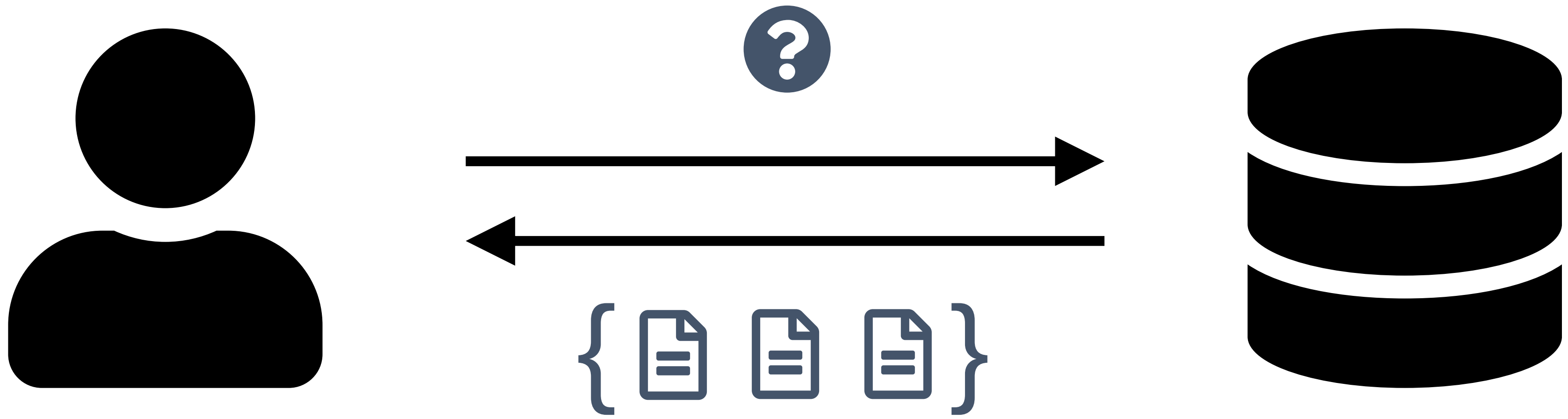
Model



unique row IDs

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

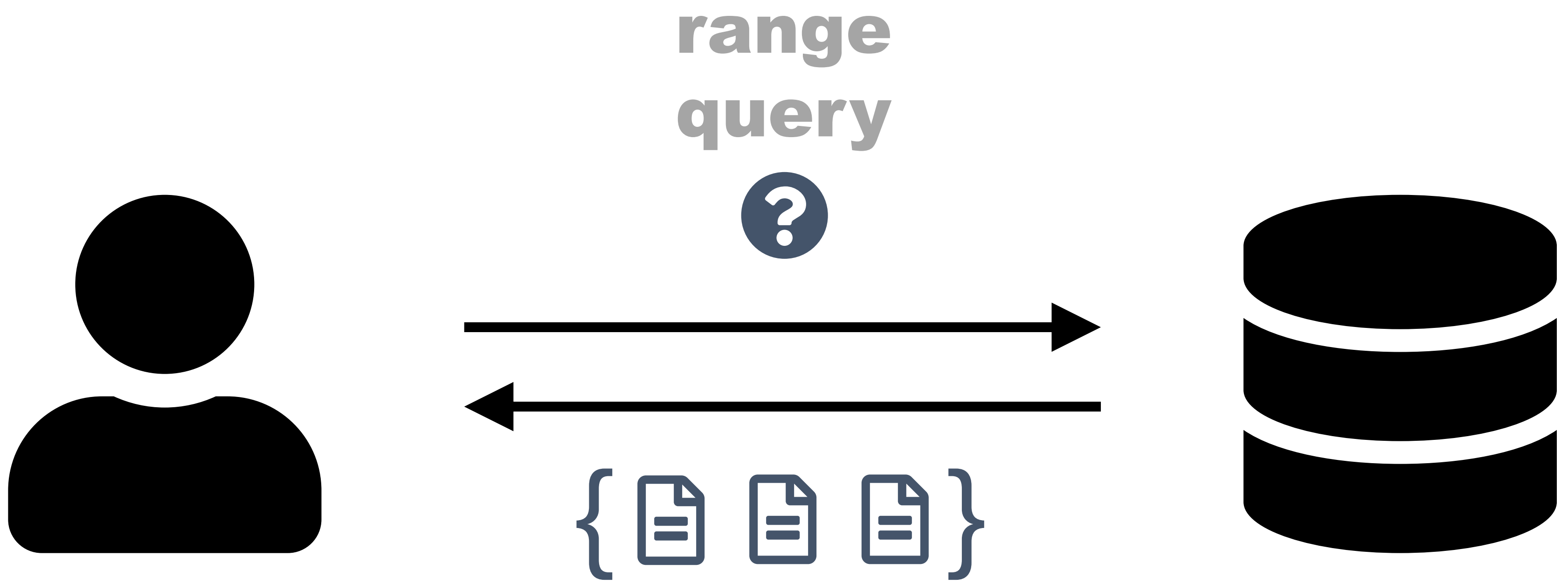
Model



numbers in {1, ..., N}

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
...	...	...

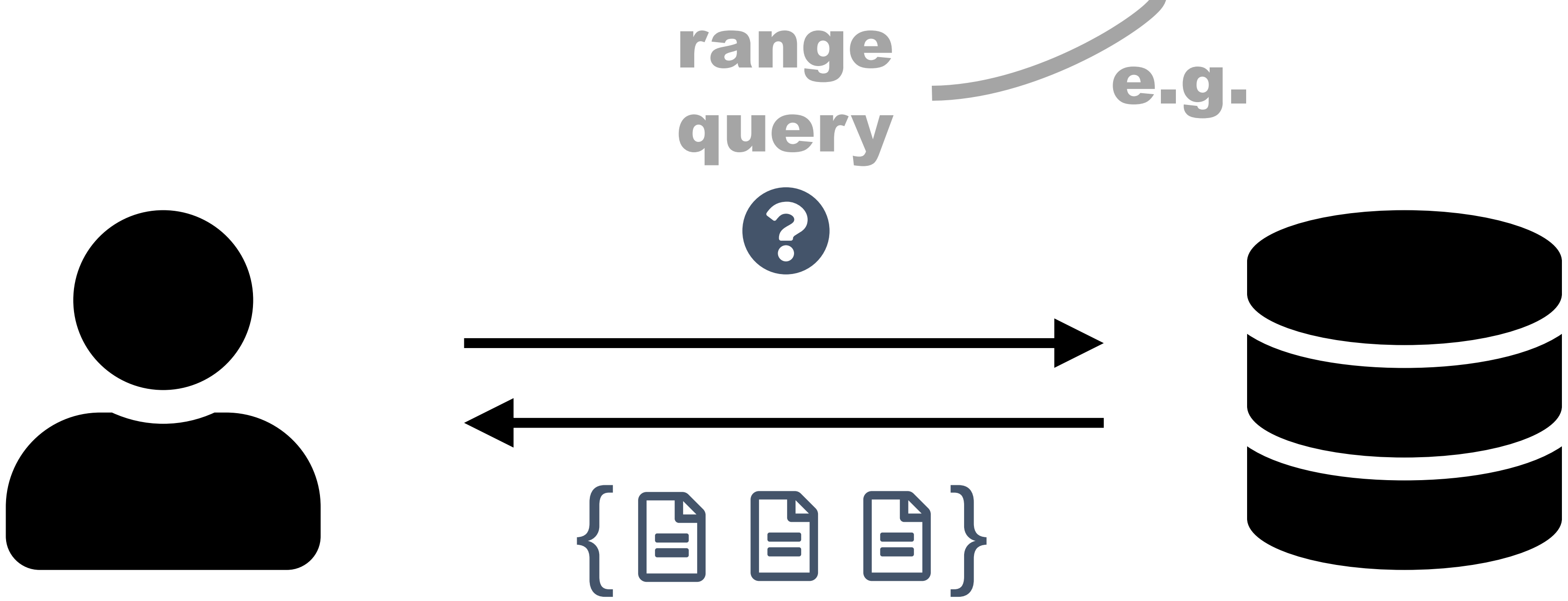
Model



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

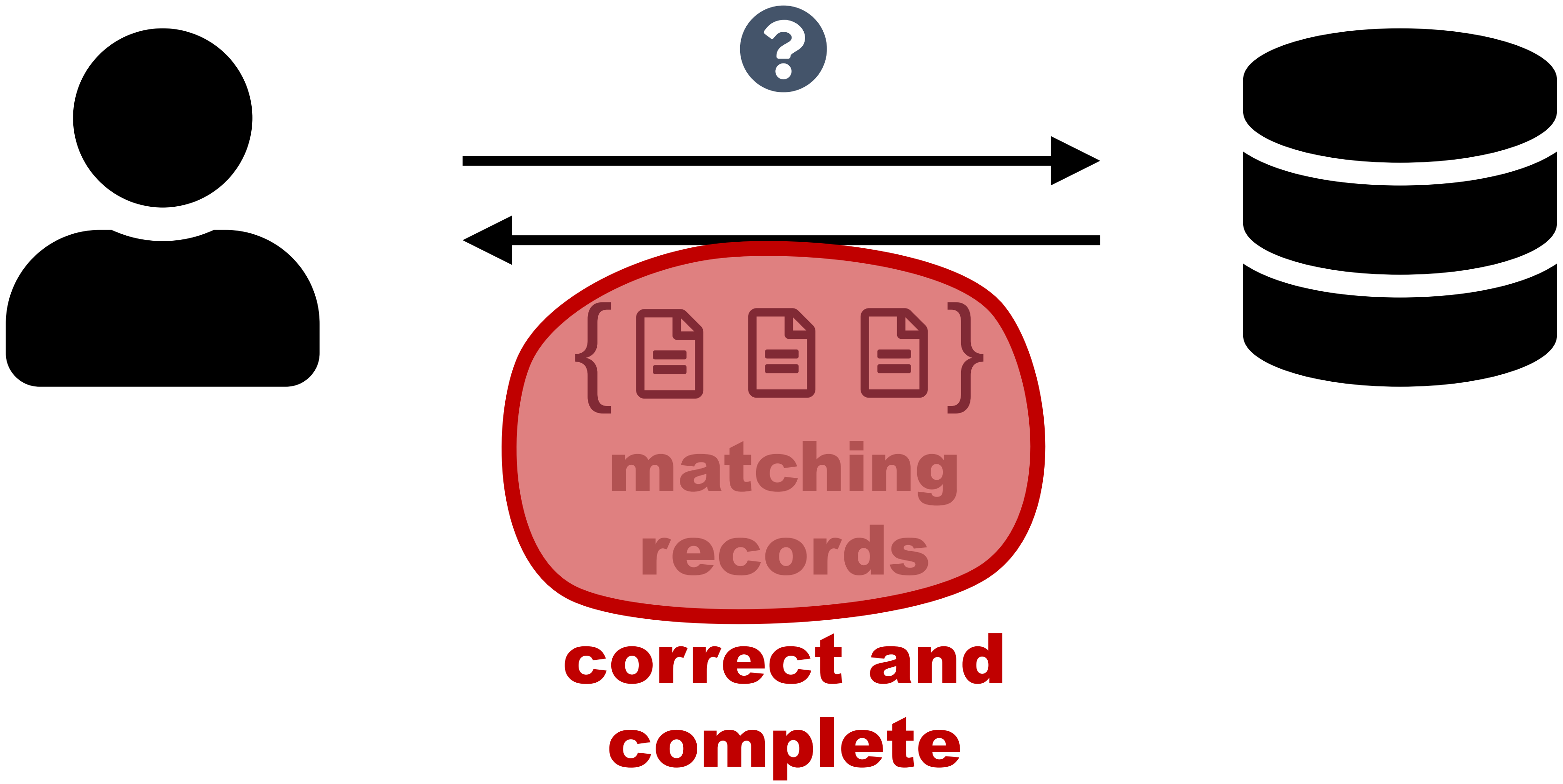
Model

```
SELECT * FROM table
WHERE Value BETWEEN X AND Y;
```



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

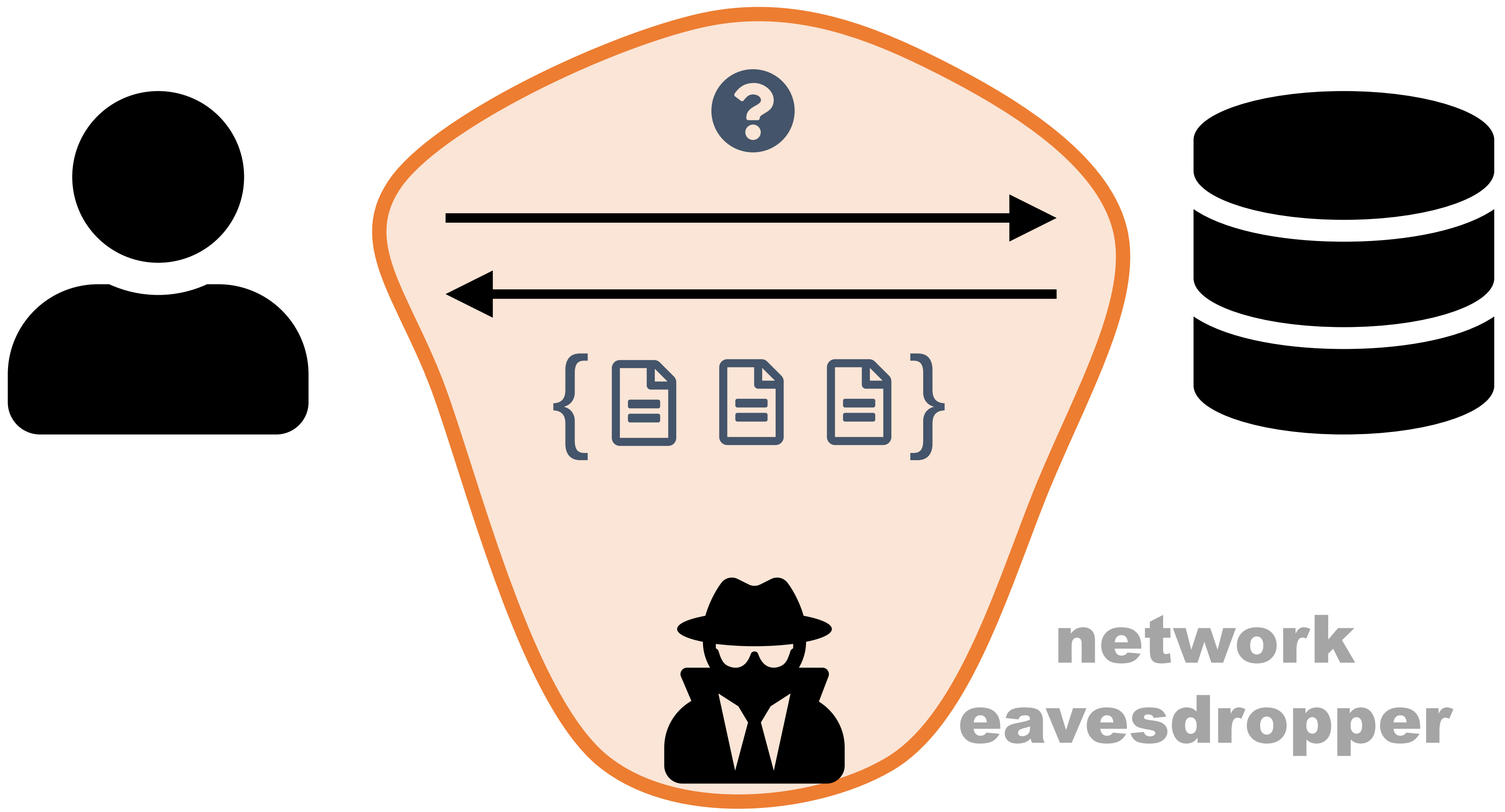
Model



numbers in {1, ..., N}

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
...	...	...

Encrypting Data in Transit

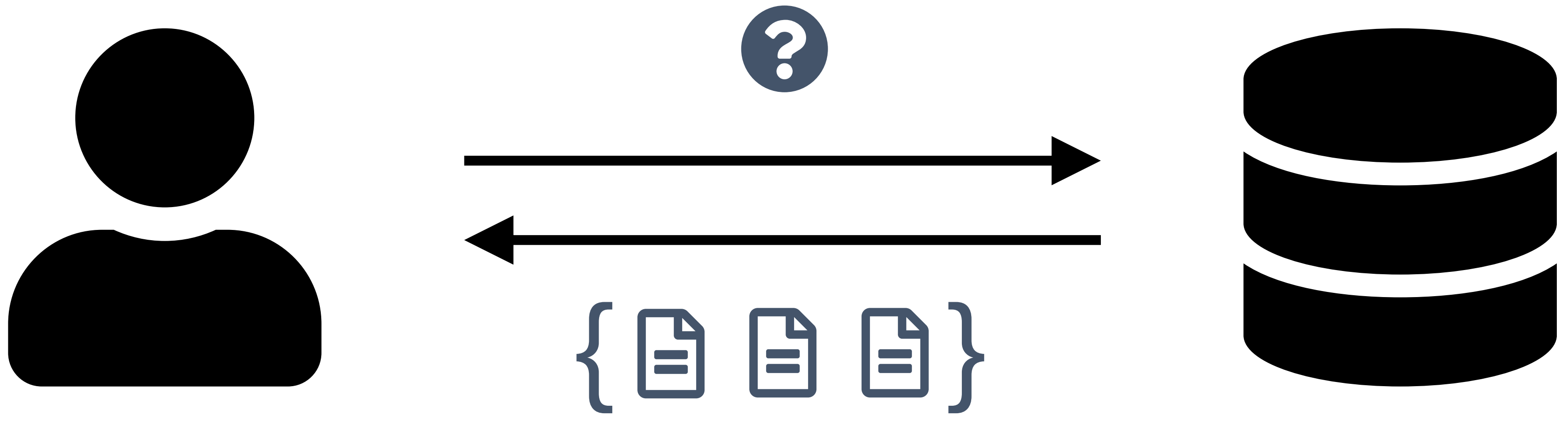


	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypting Data in Transit

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

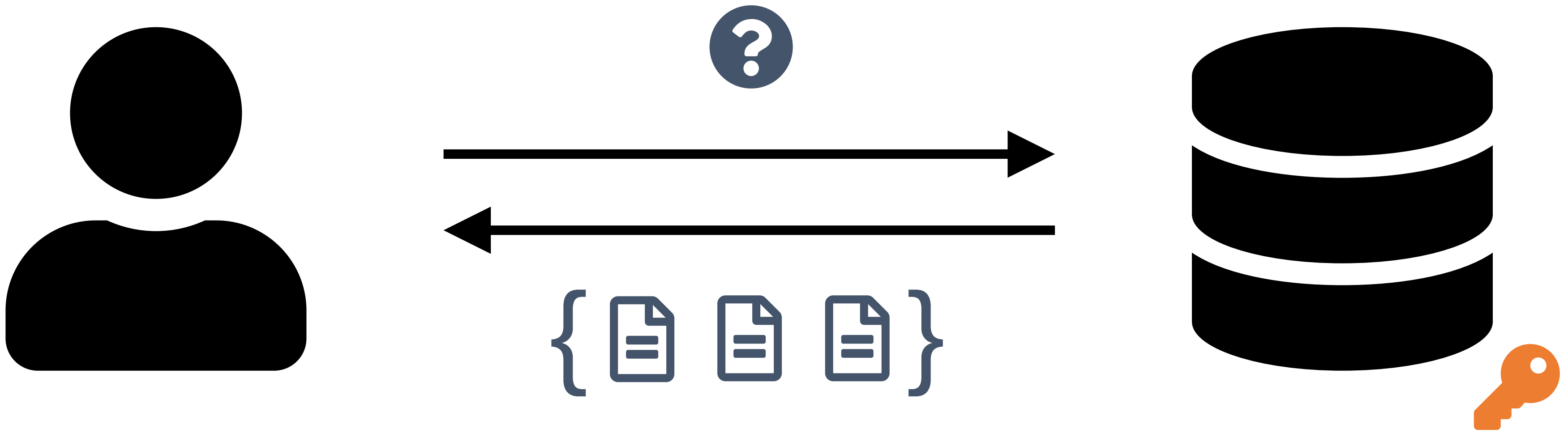
Encrypting Data at Rest



disk thief

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

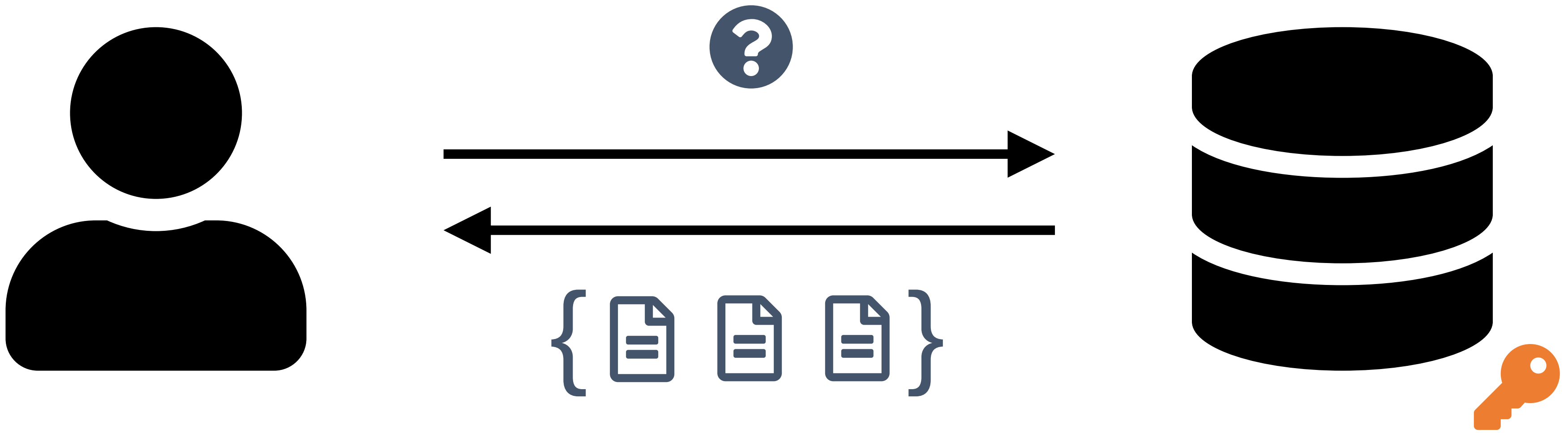
Encrypting Data at Rest

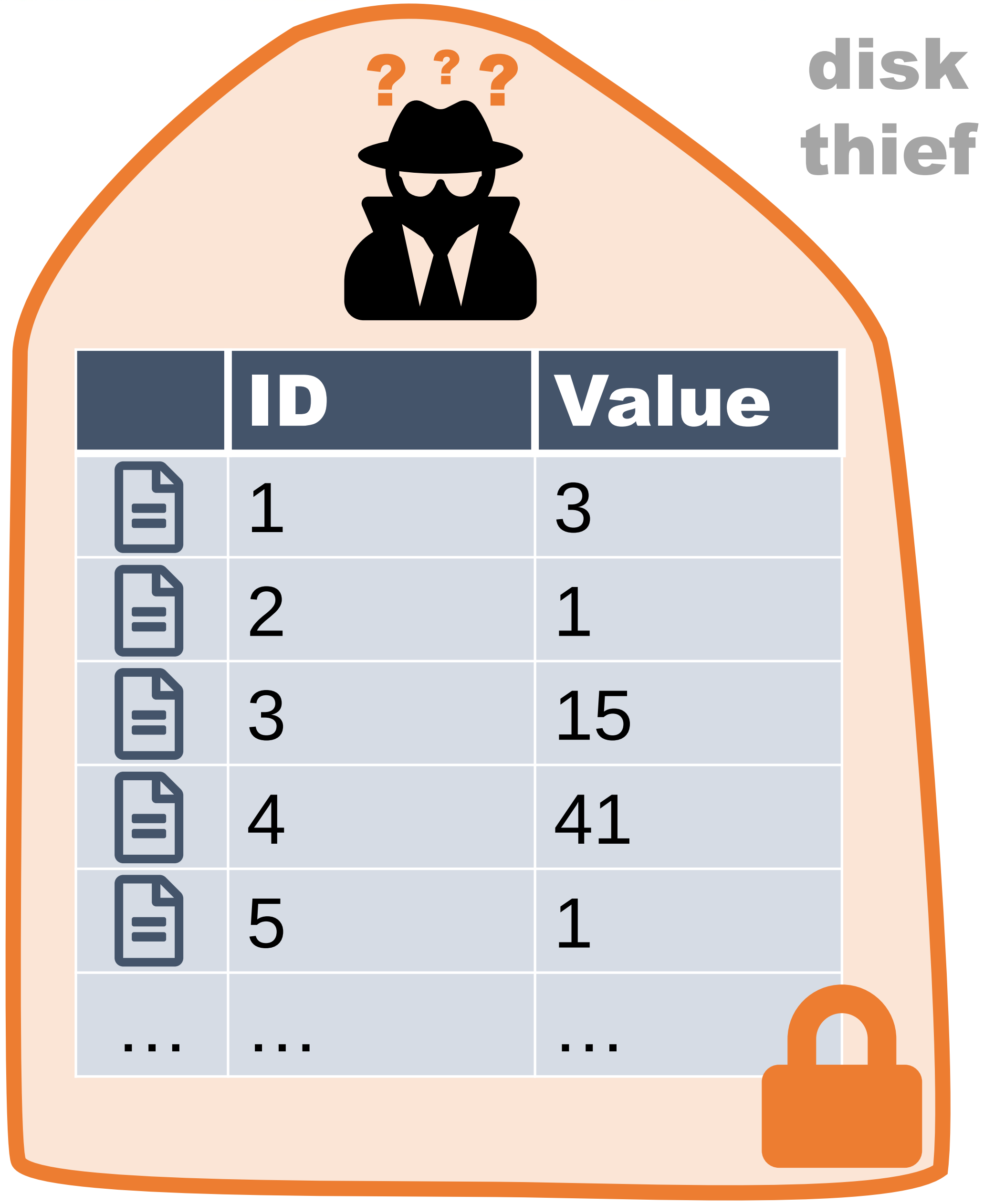


disk
thief

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

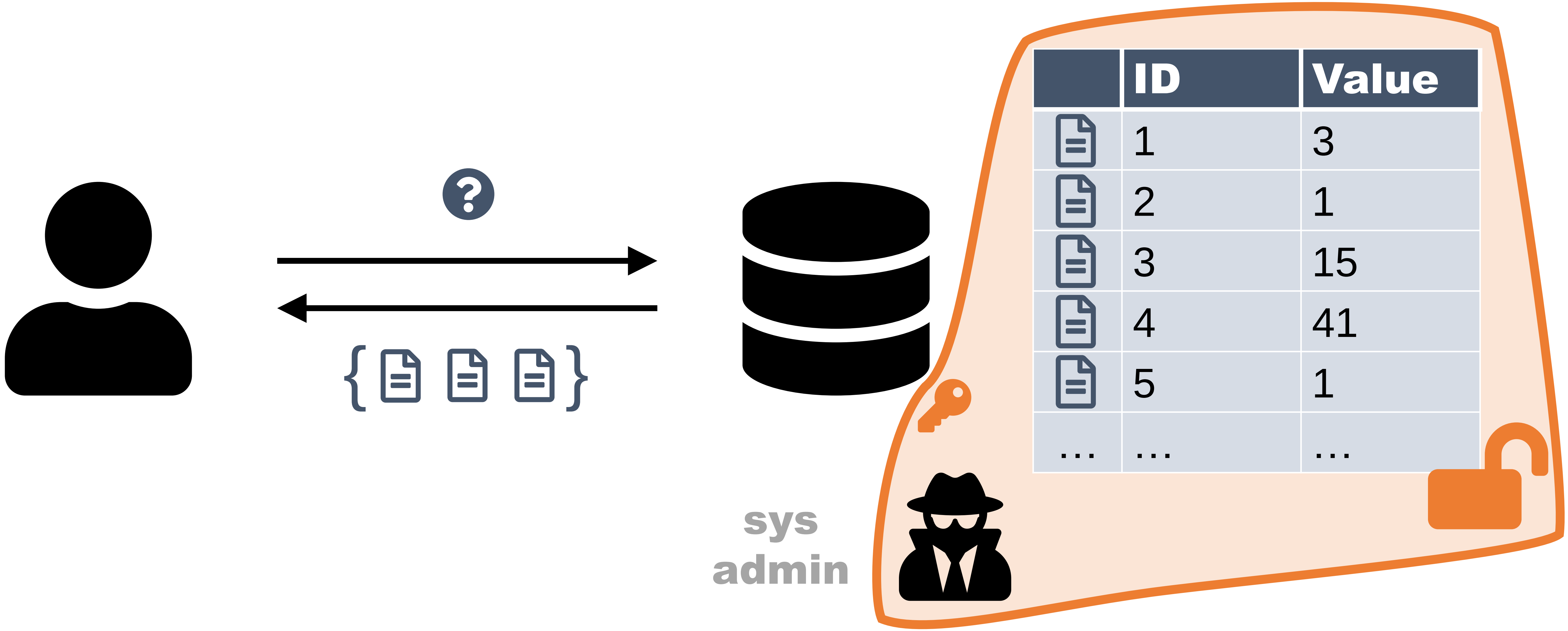
Encrypting Data at Rest





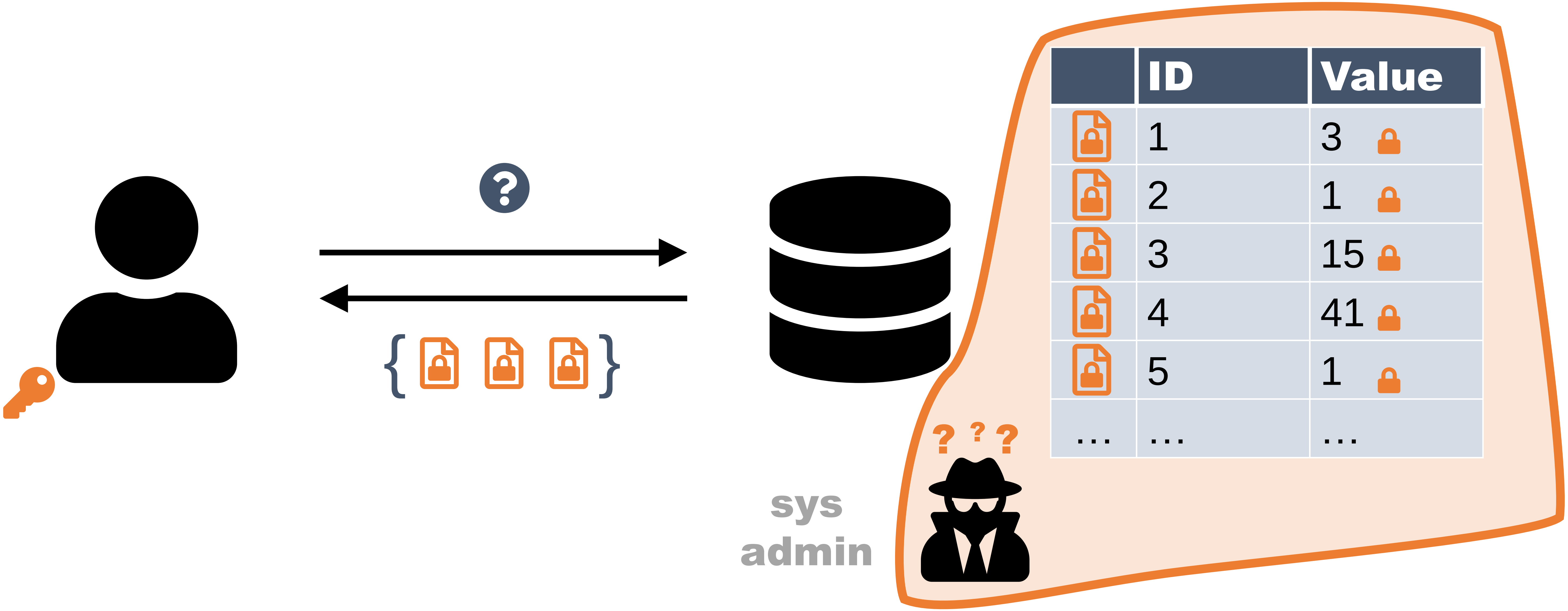
	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypting Data at Rest



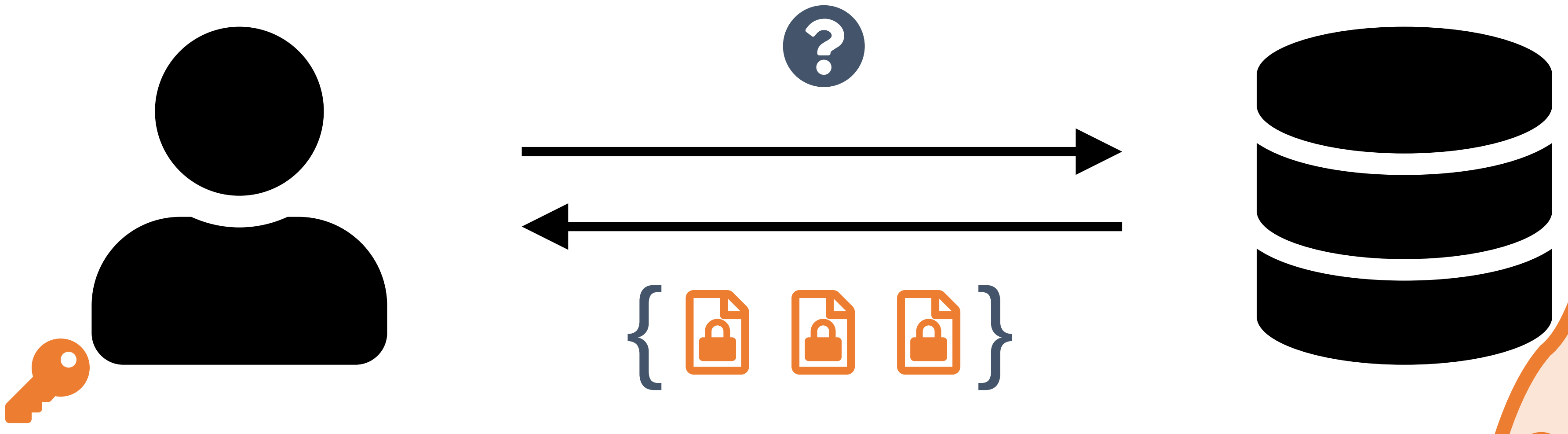
	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypting Data Client-side



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypting Data Client-side



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

sys admin

Encrypting Data Client-side

PLAINTEXT

ID	Value
1	3
2	1
3	15
4	41
5	1
…	…

DETERMINISTIC ENCRYPTION

ID	Value
1	0x18fa83
2	0x5449a1
3	0x8b7630
4	0x10cae8
5	0x5449a1
…	…

RANDOMIZED ENCRYPTION

ID	Value
1	0x5239fb
2	0x8e9d98
3	0x5a9f2e
4	0x4ff8e1
5	0xe89cfb
…	…

Encrypting Data Client-side

PLAINTEXT

ID	Value
1	3
2	1
3	15
4	41
5	1
…	…

DETERMINISTIC ENCRYPTION

ID	Value
1	0x18fa83
2	0x5449a1
3	0x8b7630
4	0x10cae8
5	0x5449a1
…	…

≠

RANDOMIZED ENCRYPTION

ID	Value
1	0x5239fb
2	0x8e9d98
3	0x5a9f2e
4	0x4ff8e1
5	0xe89cfb
…	…

Encrypting Data Client-side

DETERMINISTIC ENCRYPTION

ID	Value
1	0x18fa83
2	0x5449a1
3	0x8b7630
4	0x10cae8
5	0x5449a1
…	…

- Range queries are possible:

  `... WHERE Value BETWEEN 1 AND 3`

  becomes

  `... WHERE Value IN`

  `(Enc(1), Enc(2), Enc(3))`

- Revealing repeated values is dangerous

  [Naveed et al., CCS 2015]

Encrypting Data Client-side

PLAINTEXT

ID	Value
1	3
2	1
3	15
4	41
5	1
…	…

DETERMINISTIC ENCRYPTION

ID	Value
1	0x18fa83
2	0x5449a1
3	0x8b7630
4	0x10cae8
5	0x5449a1
…	…

RANDOMIZED ENCRYPTION

ID	Value
1	0x5239fb
2	0x8e9d98
3	0x5a9f2e
4	0x4ff8e1
5	0xe89cfb
…	…

$\neq$

range queries impossible

Encrypting Data Client-side

PLAINTEXT

ID	Value
1	3
2	1
3	15
4	41
5	1
…	…

1 < 15

ORDER-PRESERVING ENCRYPTION

ID	Value
1	182
2	84
3	2307
4	8932
5	84
…	…

84 < 2307

[Agrawal et al., SIGMOD 2004],
[Boldyreva et al., EUROCRYPT 2009]

Encrypting Data Client-side

- "Ideal" OPE leaks approximate value and distance
  [Boldyreva et al., CRYPTO 2011]

- Revealing repeated values is even more dangerous
  [Naveed et al., CCS 2015]
  [Grubbs et al., S&P 2017]

ORDER-PRESERVING ENCRYPTION

ID	Value
1	182
2	84
3	2307
4	8932
5	84
…	…

Encrypting Data Client-side

- Order-Revealing Encryption (ORE)

[Chenette et al., FSE 2016],
[Lewi and Wu, CCS 2016]

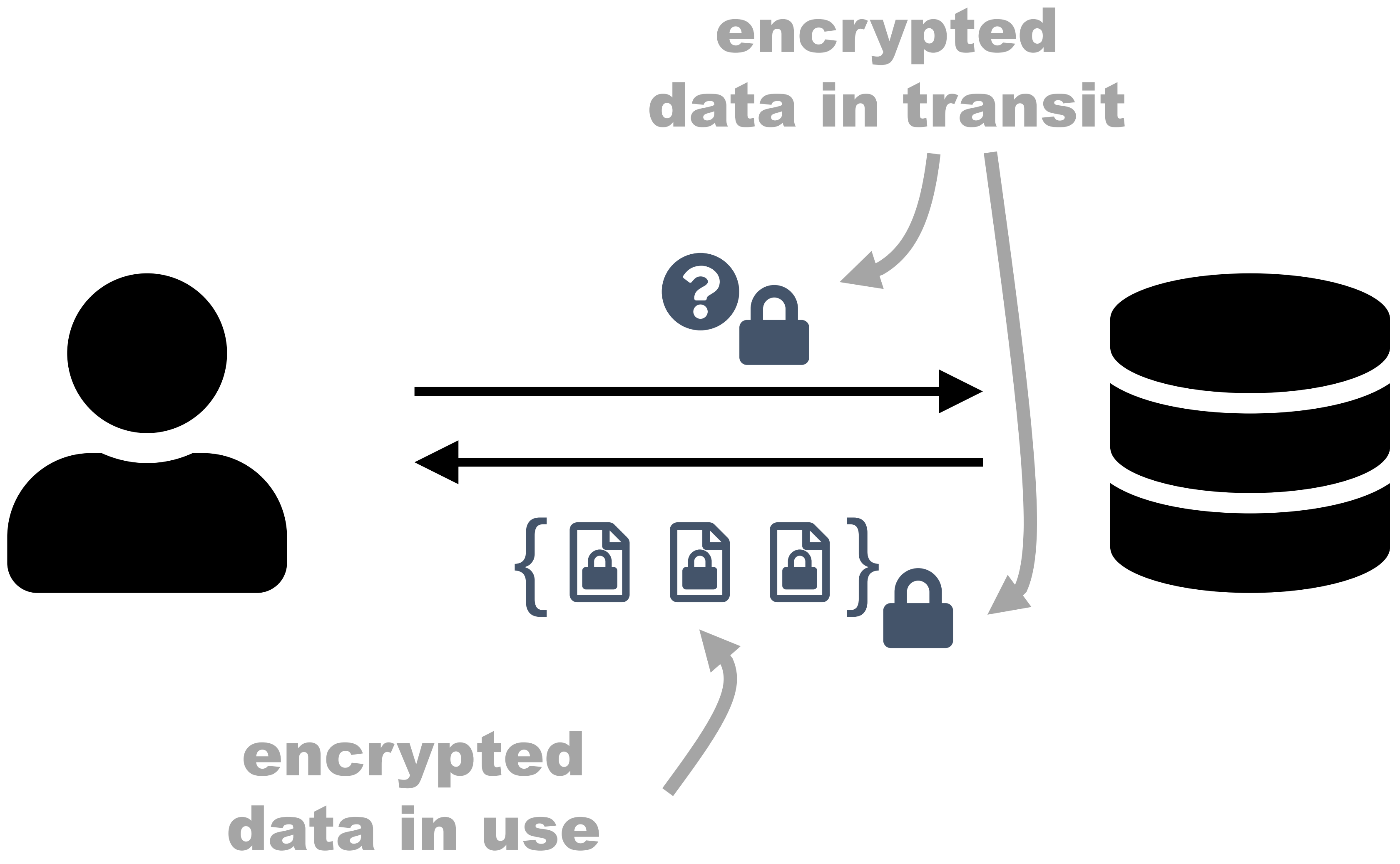
- Partial Order-Preserving Encoding

[Roche et al., CCS 2016]

- Custom search indices

[Boelter et al., eprint 2016/568]

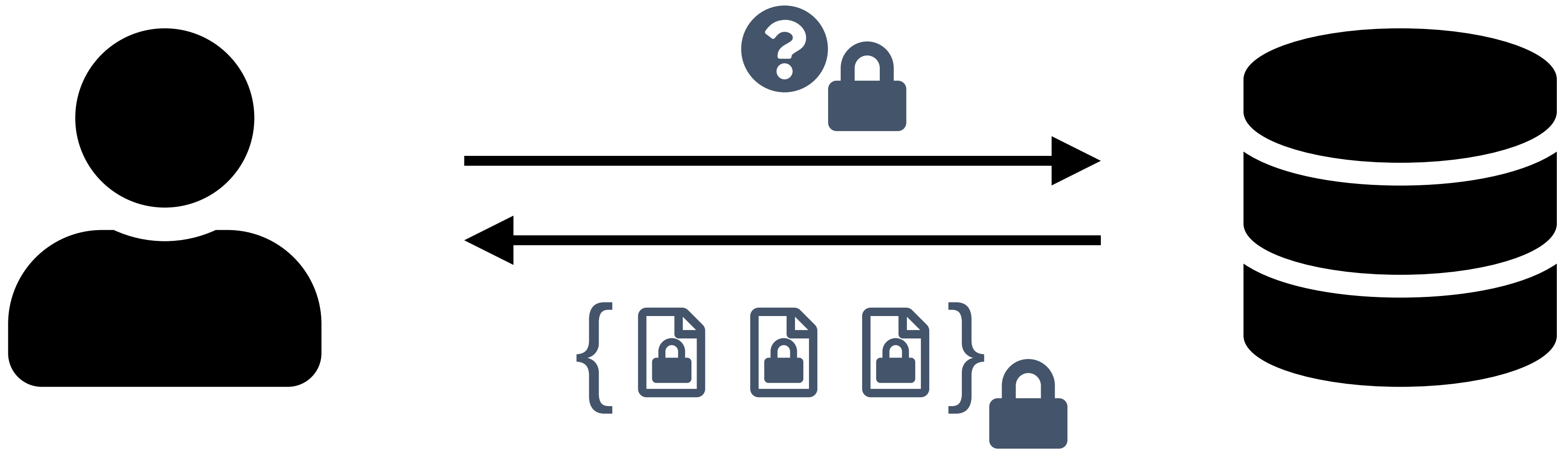
Encrypting Everything



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

encrypted
data at rest

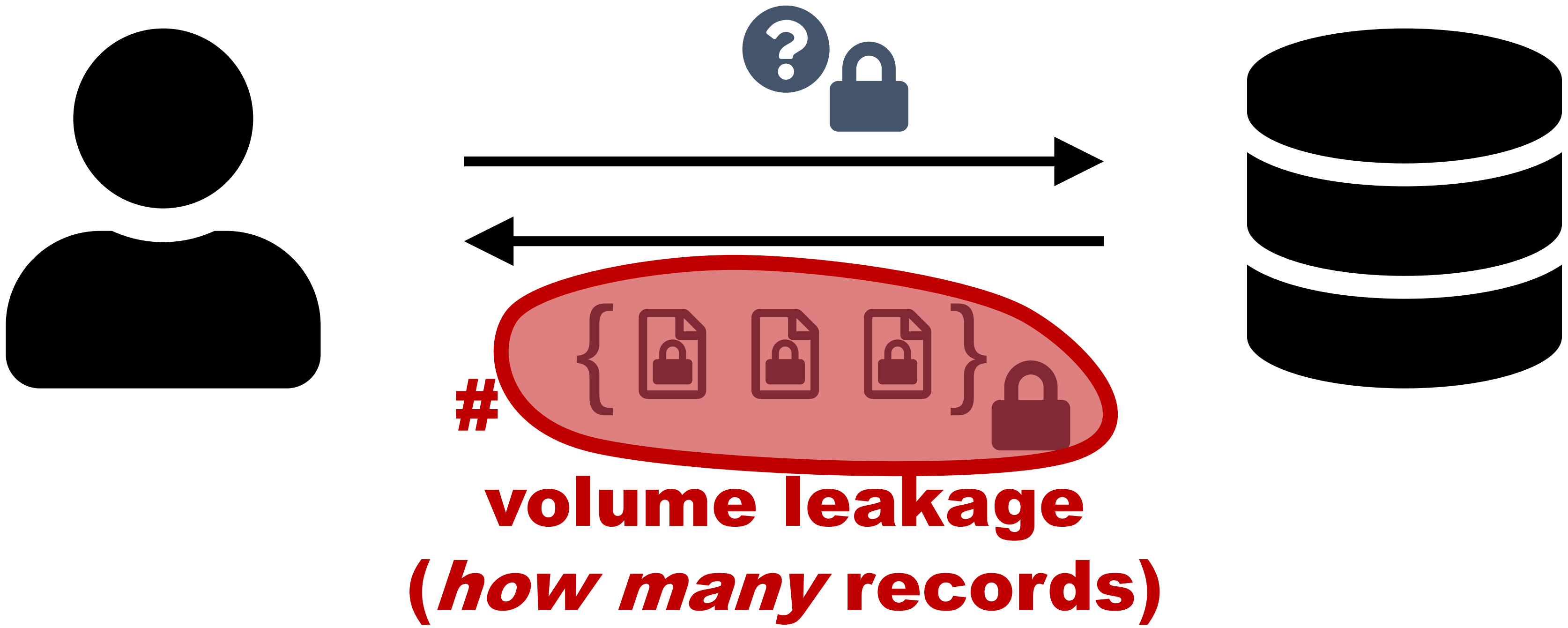
Encrypting Everything



access pattern leakage (*which* records)

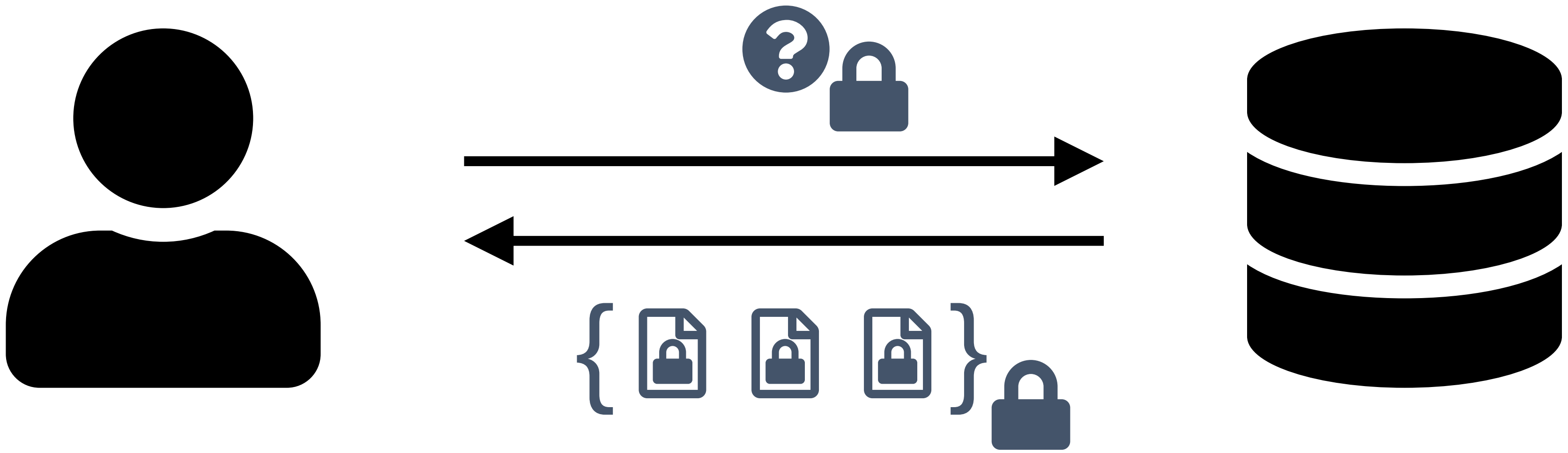
	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypting Everything



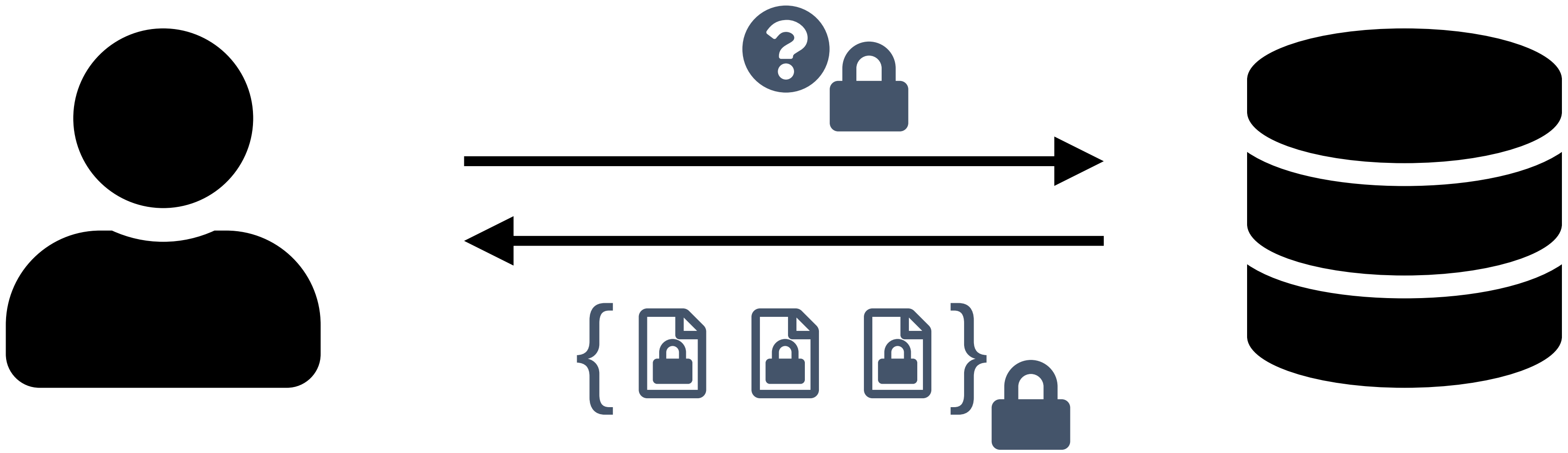
	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypting Everything



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypting Everything



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

[Grubbs et al., HotOS 2017]

Existing Approaches

- No fixed definition of "encrypted database"
- Encryption mitigates threats (network, theft, server compromise)
- Despite these solutions, access pattern and volume can leak

Outline

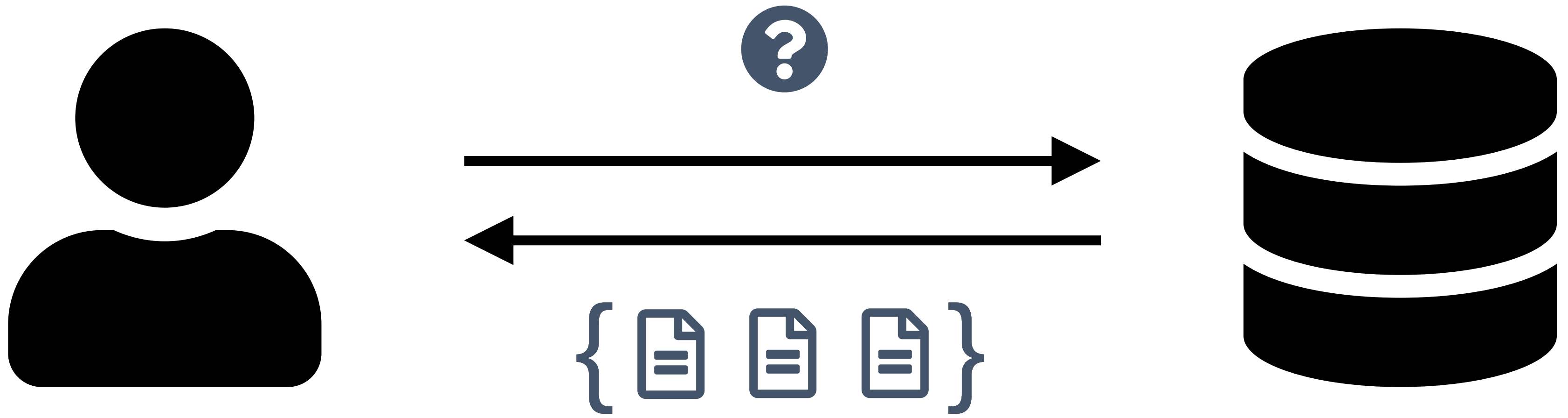
1. Existing approaches to securing a database
    - Securing data in transit, at rest, and in use

2. How to exploit leakage to break database encryption
    - Exploiting access pattern leakage and volume leakage

3. Security recommendations
    - Types of leakage, leaky operations, trade-offs

Exploiting Access Pattern Leakage

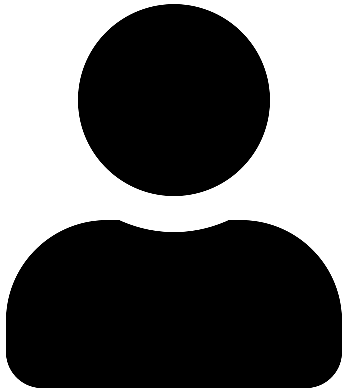
```
SELECT * FROM table
WHERE Value BETWEEN ? AND ?;
```

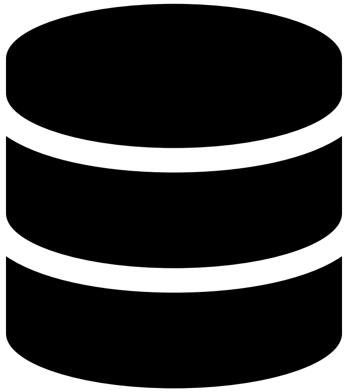


	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

{ 1, 2, 5 }

Example





	ID	Value
	1	0x5239fb
	2	0x8e9d98
	3	0x5a9f2e
	4	0x4ff8e1
	5	0xe89cfb
	6	0x4073d2
	7	0x2765be
	8	0x74090f
	9	0x5bae94
	10	0xae60da

Query 1

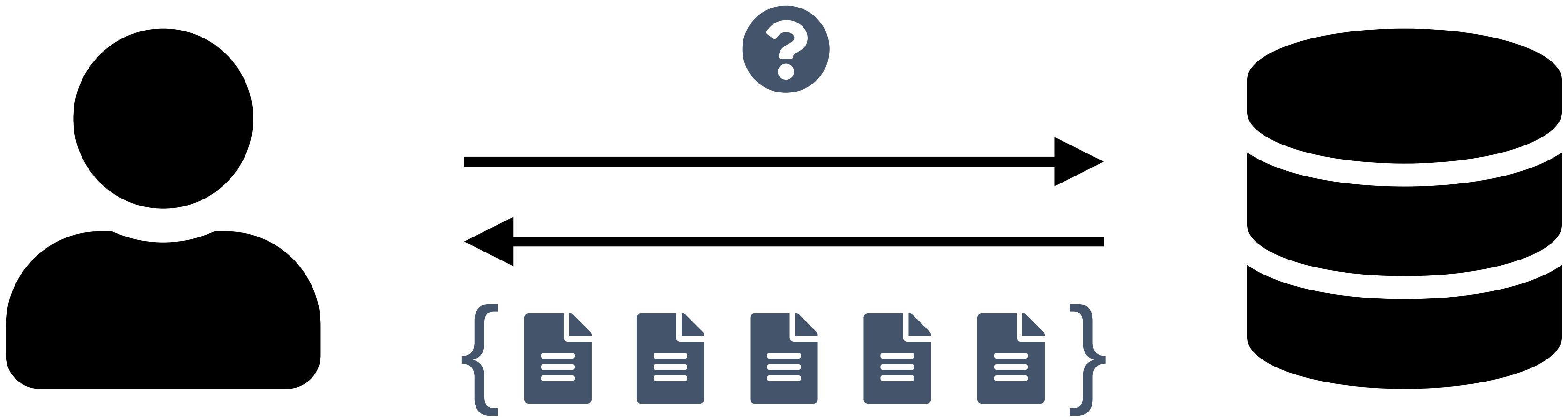
```
SELECT * FROM table
WHERE Value BETWEEN ? AND ?;
```

	ID	Value
	1	0x5239fb
	2	0x8e9d98
	3	0x5a9f2e
	4	0x4ff8e1
	5	0xe89cfb
	6	0x4073d2
	7	0x2765be
	8	0x74090f
	9	0x5bae94
	10	0xae60da

{2, 3, 5, 10}

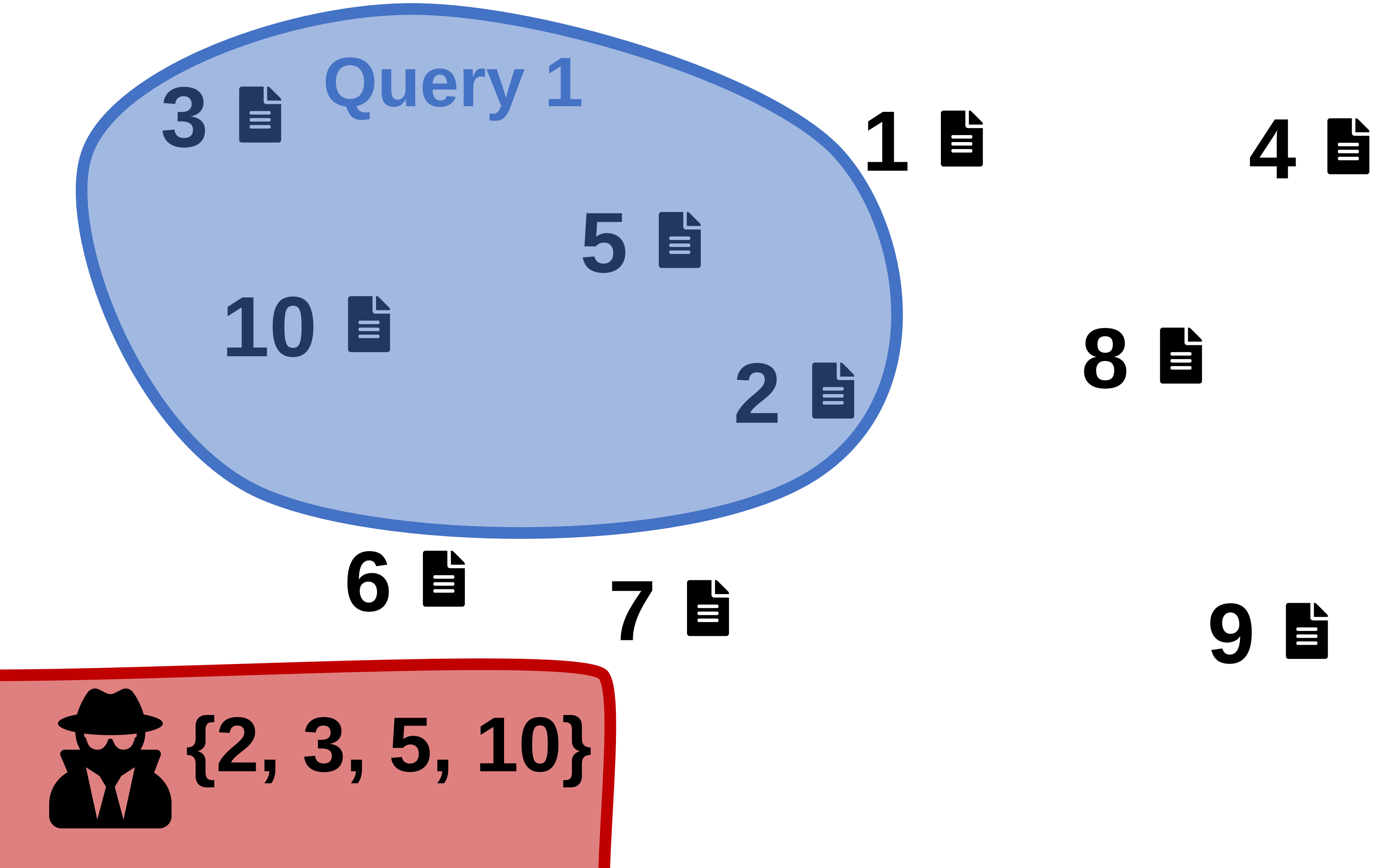
Query 2

```
SELECT * FROM table
WHERE Value BETWEEN ? AND ?;
```

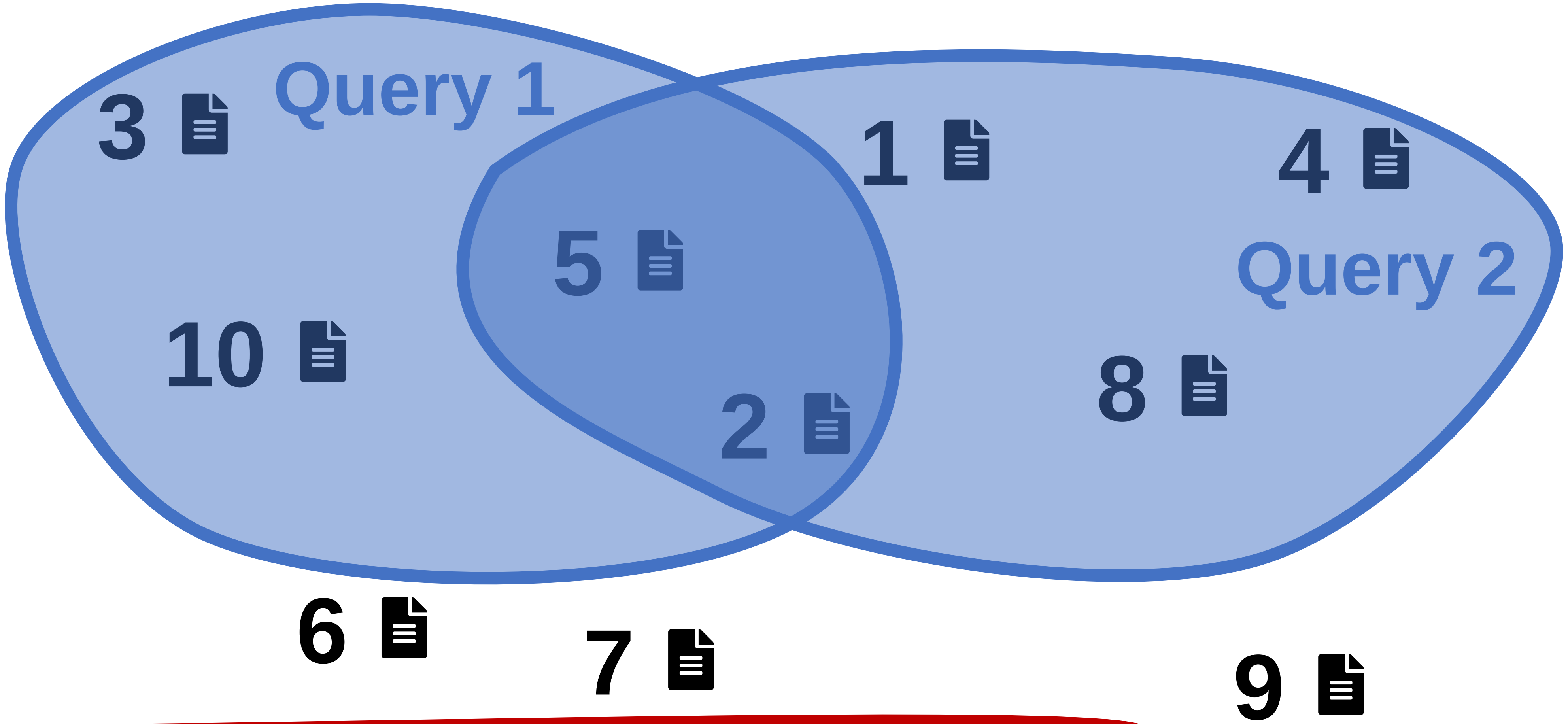


{2, 3, 5, 10}, {1, 2, 4, 5, 8}

	ID	Value
	1	0x5239fb
	2	0x8e9d98
	3	0x5a9f2e
	4	0x4ff8e1
	5	0xe89cfb
	6	0x4073d2
	7	0x2765be
	8	0x74090f
	9	0x5bae94
	10	0xae60da

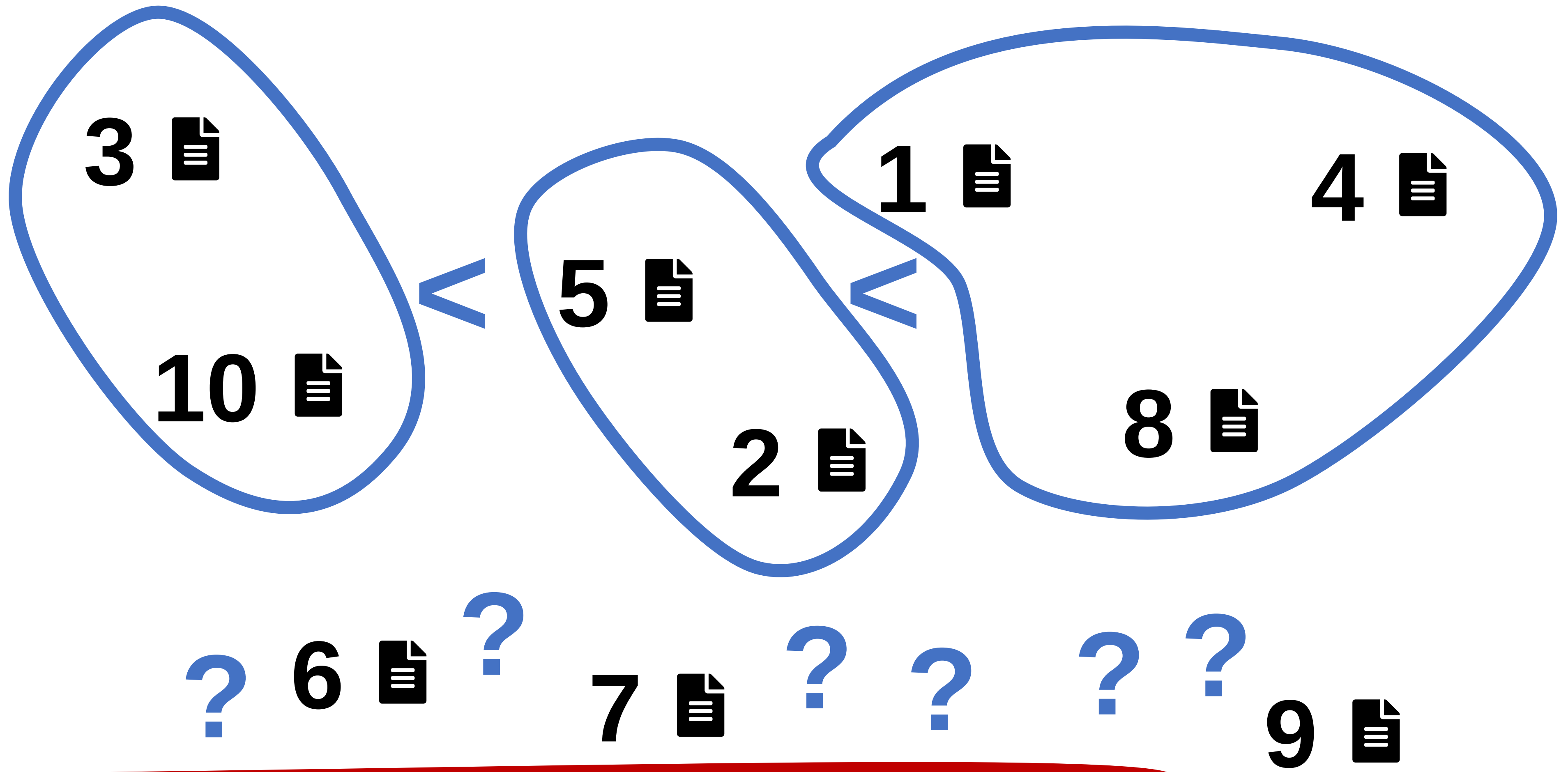


	ID	Value
	1	0x5239fb
	2	0x8e9d98
	3	0x5a9f2e
	4	0x4ff8e1
	5	0xe89cfb
	6	0x4073d2
	7	0x2765be
	8	0x74090f
	9	0x5bae94
	10	0xae60da



	ID	Value
	1	0x5239fb
	2	0x8e9d98
	3	0x5a9f2e
	4	0x4ff8e1
	5	0xe89cfb
	6	0x4073d2
	7	0x2765be
	8	0x74090f
	9	0x5bae94
	10	0xae60da

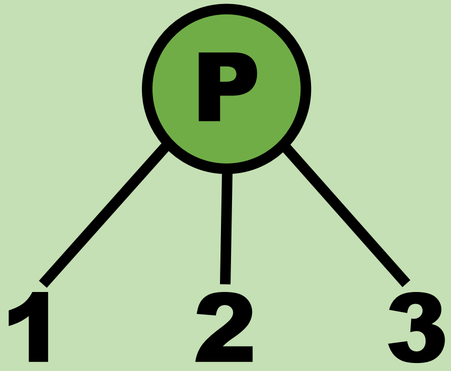
{2, 3, 5, 10}, {1, 2, 4, 5, 8}



{2, 3, 5, 10}, {1, 2, 4, 5, 8}

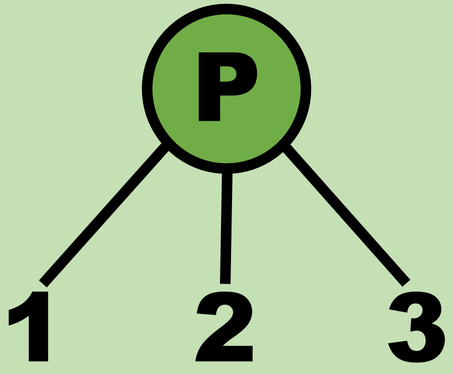
	ID	Value
	1	0x5239fb
	2	0x8e9d98
	3	0x5a9f2e
	4	0x4ff8e1
	5	0xe89cfb
	6	0x4073d2
	7	0x2765be
	8	0x74090f
	9	0x5bae94
	10	0xae60da

PQ Trees: Sets of Orderings

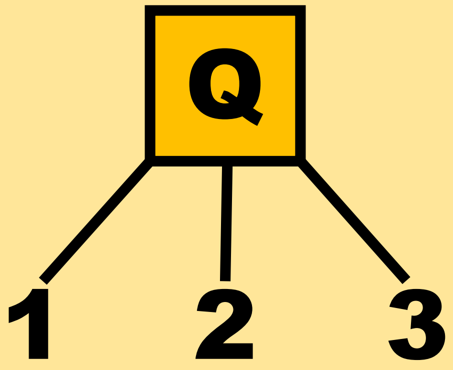


(1, 2, 3) or (1, 3, 2) or (2, 1, 3) or (2, 3, 1) or (3, 1, 2) or (3, 2, 1)

PQ Trees: Sets of Orderings



(1, 2, 3) or (1, 3, 2) or (2, 1, 3) or (2, 3, 1) or (3, 1, 2) or (3, 2, 1)

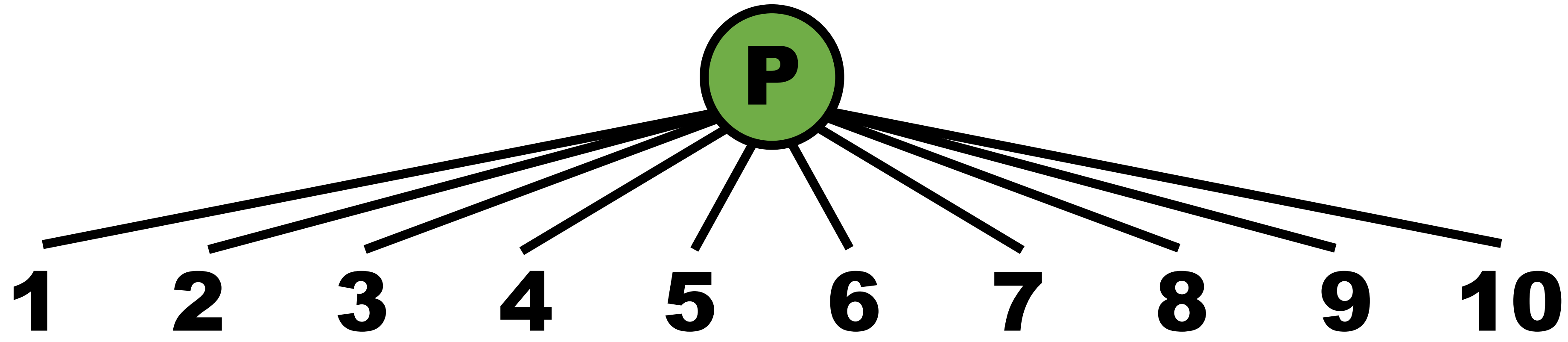


(1, 2, 3) or (3, 2, 1)

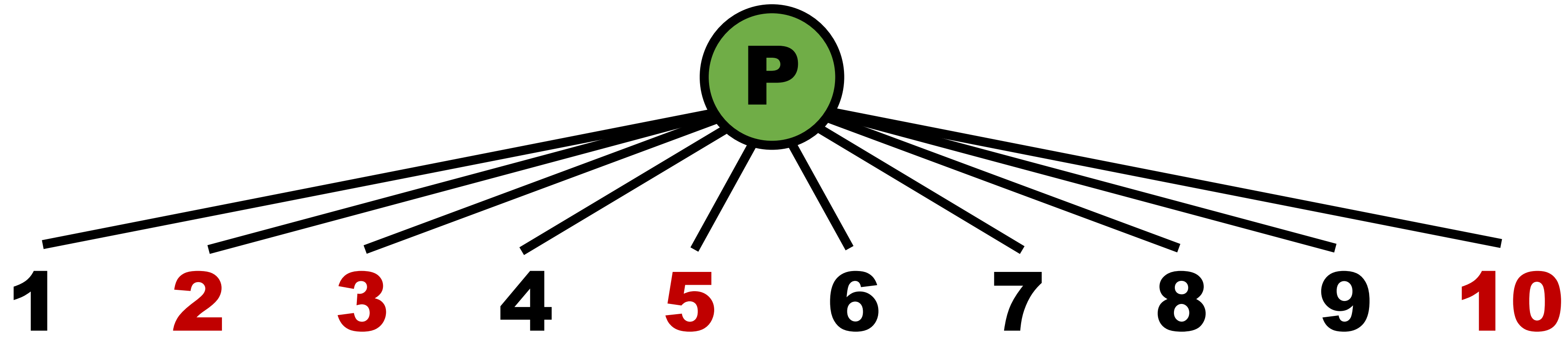
[Dautrich and Ravishankar, EDBT 2013]
[Booth and Lueker, J. Comput. Sys. Sci., 1976]

Example: Access Pattern Leakage

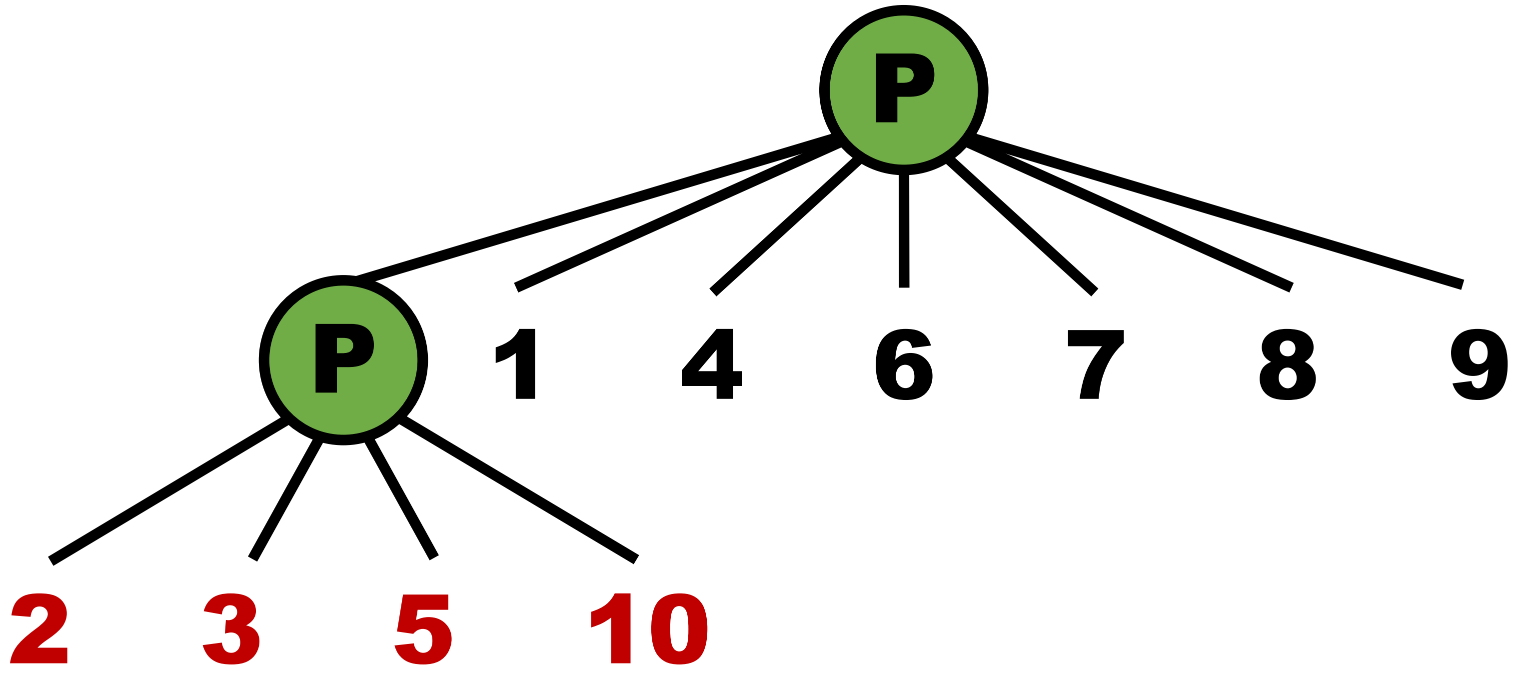
	ID	Value



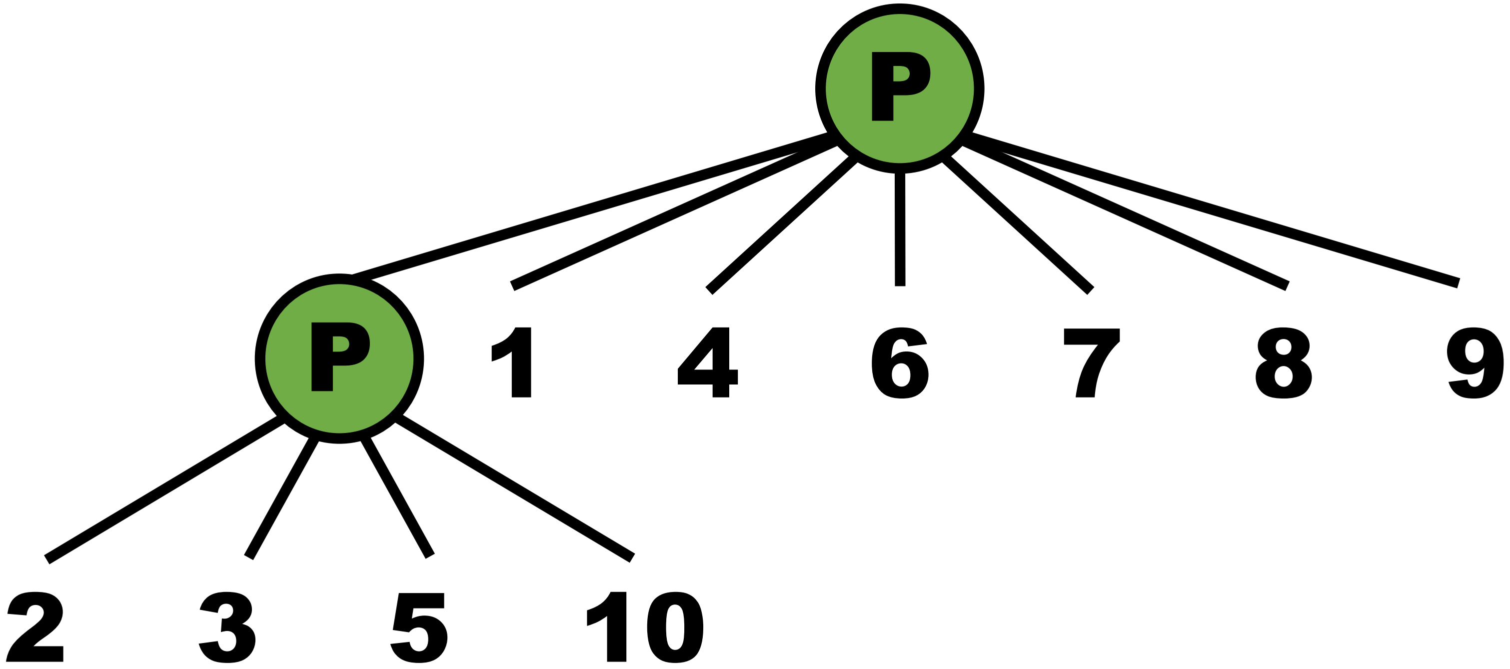
Query 1



Query 1

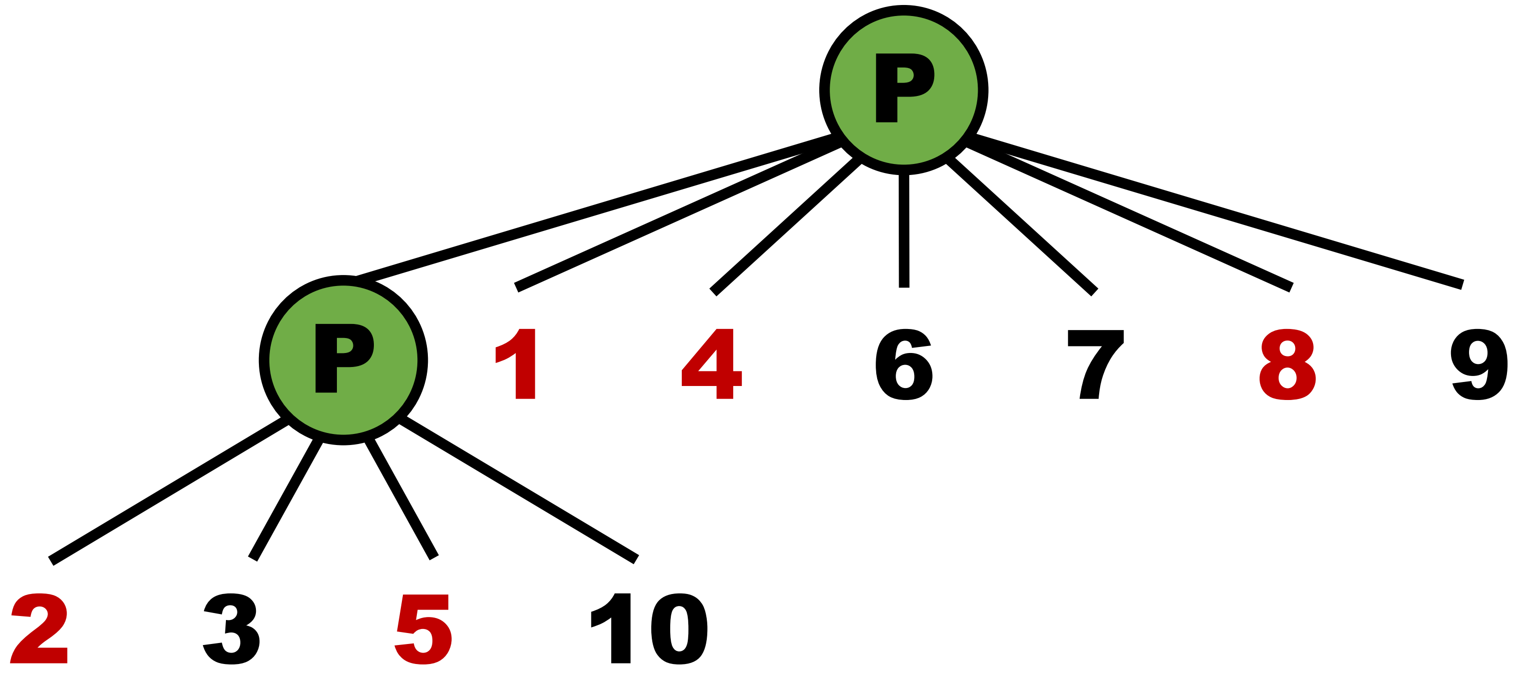


Query 1

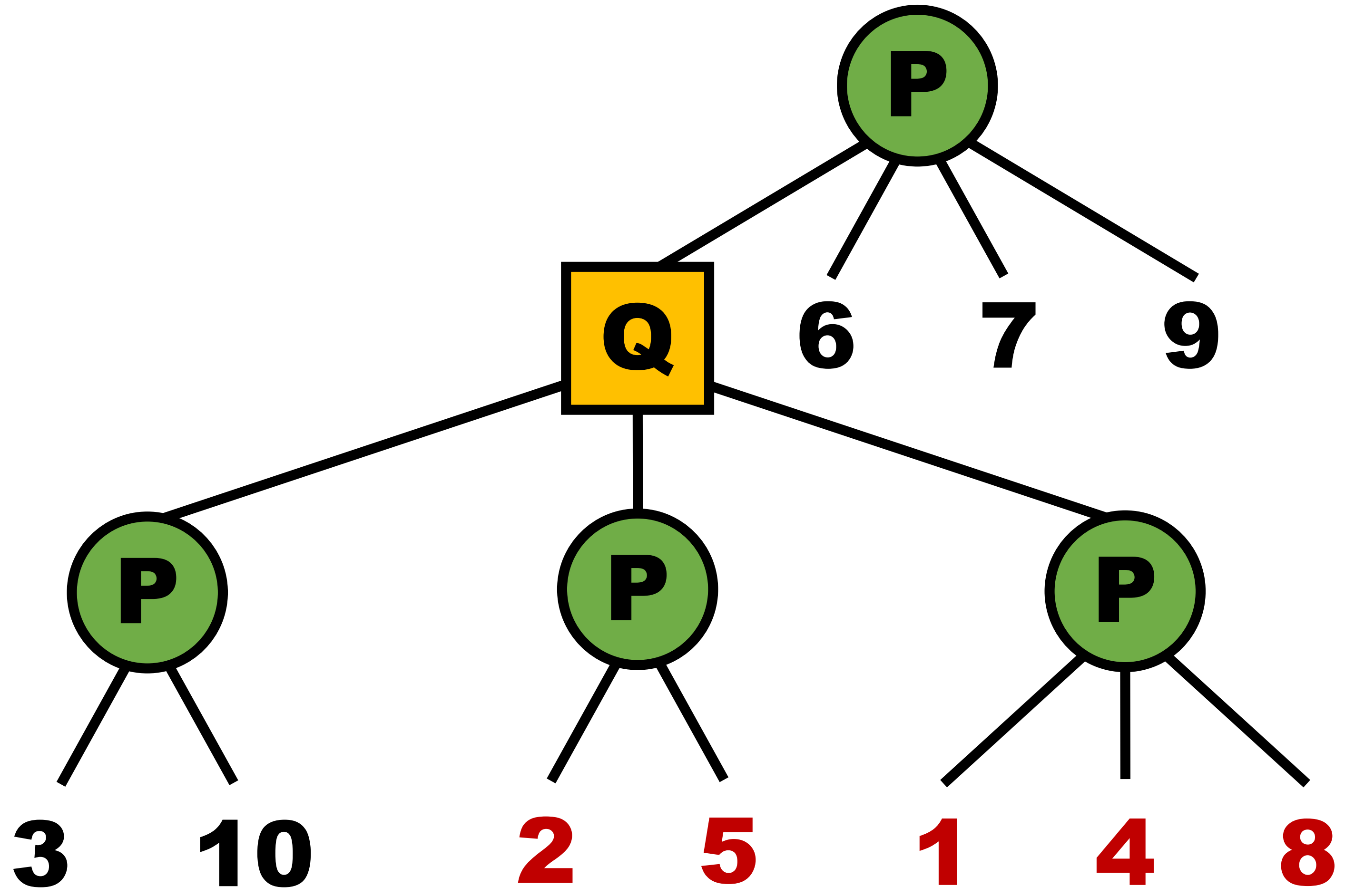


	ID	Value

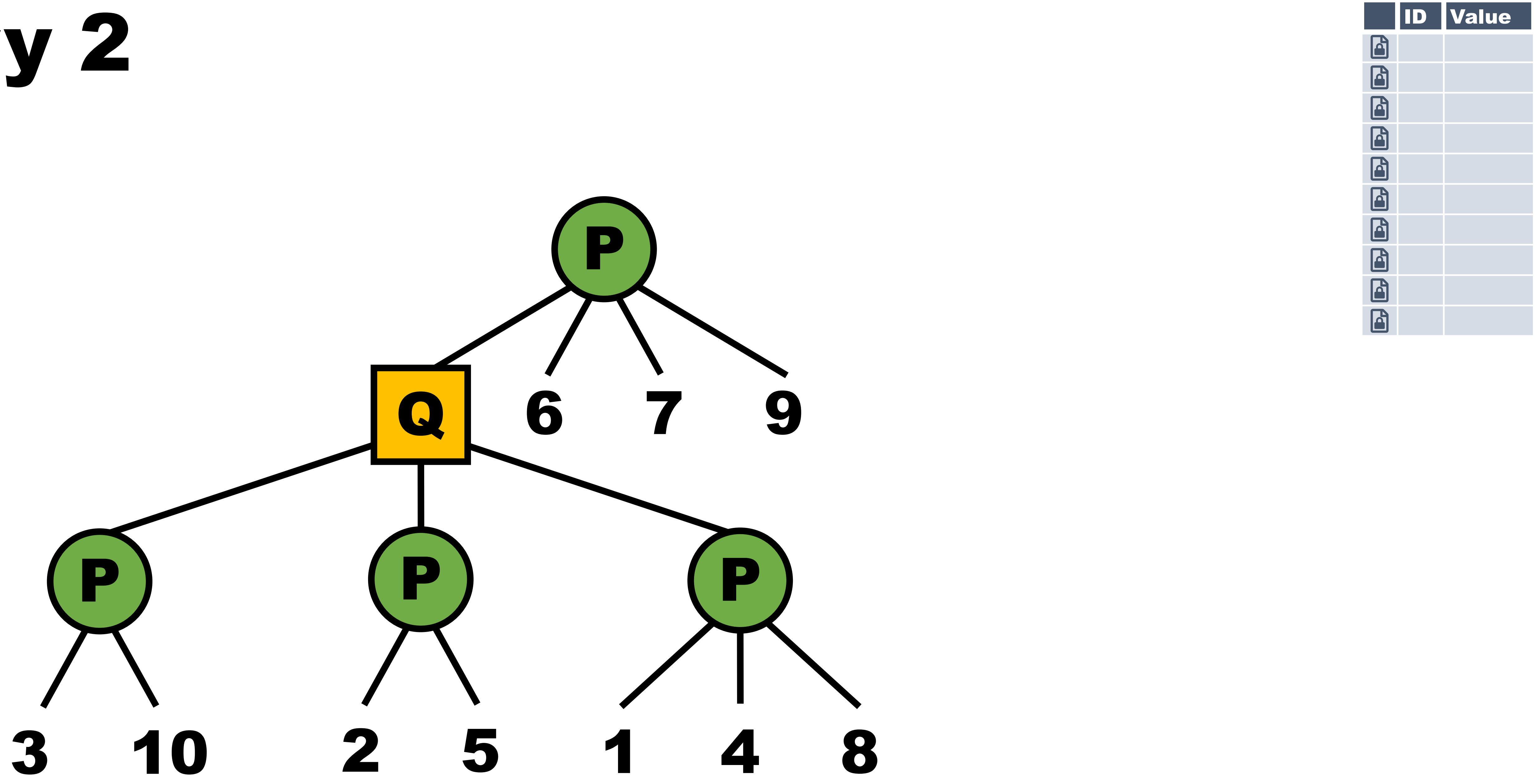
Query 2



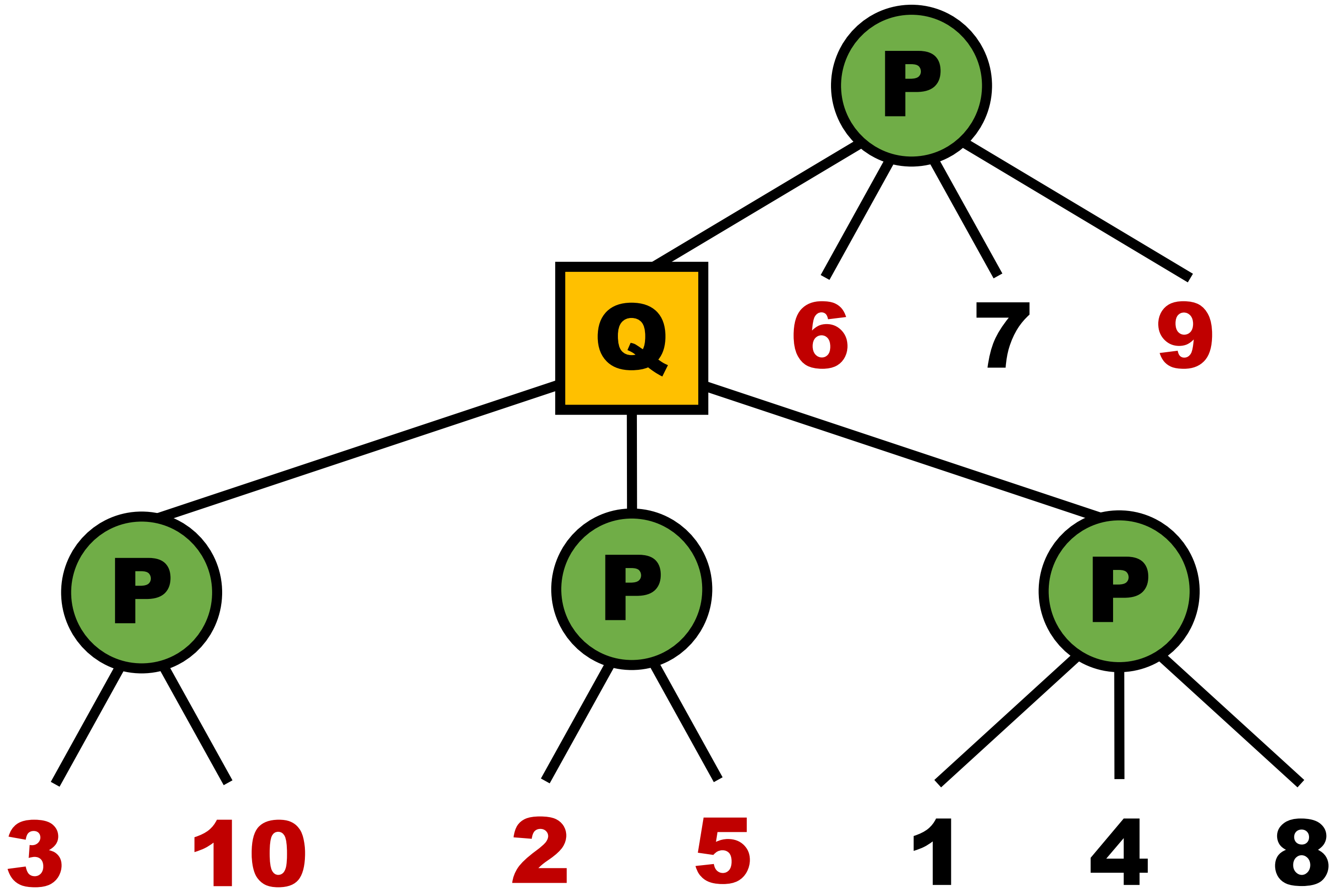
Query 2

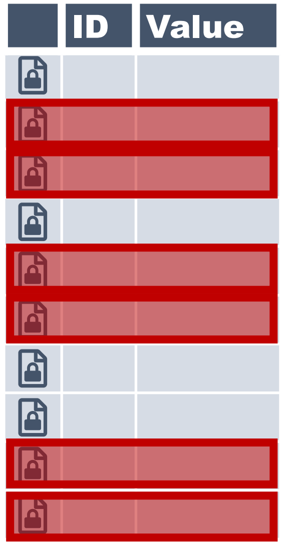


Query 2

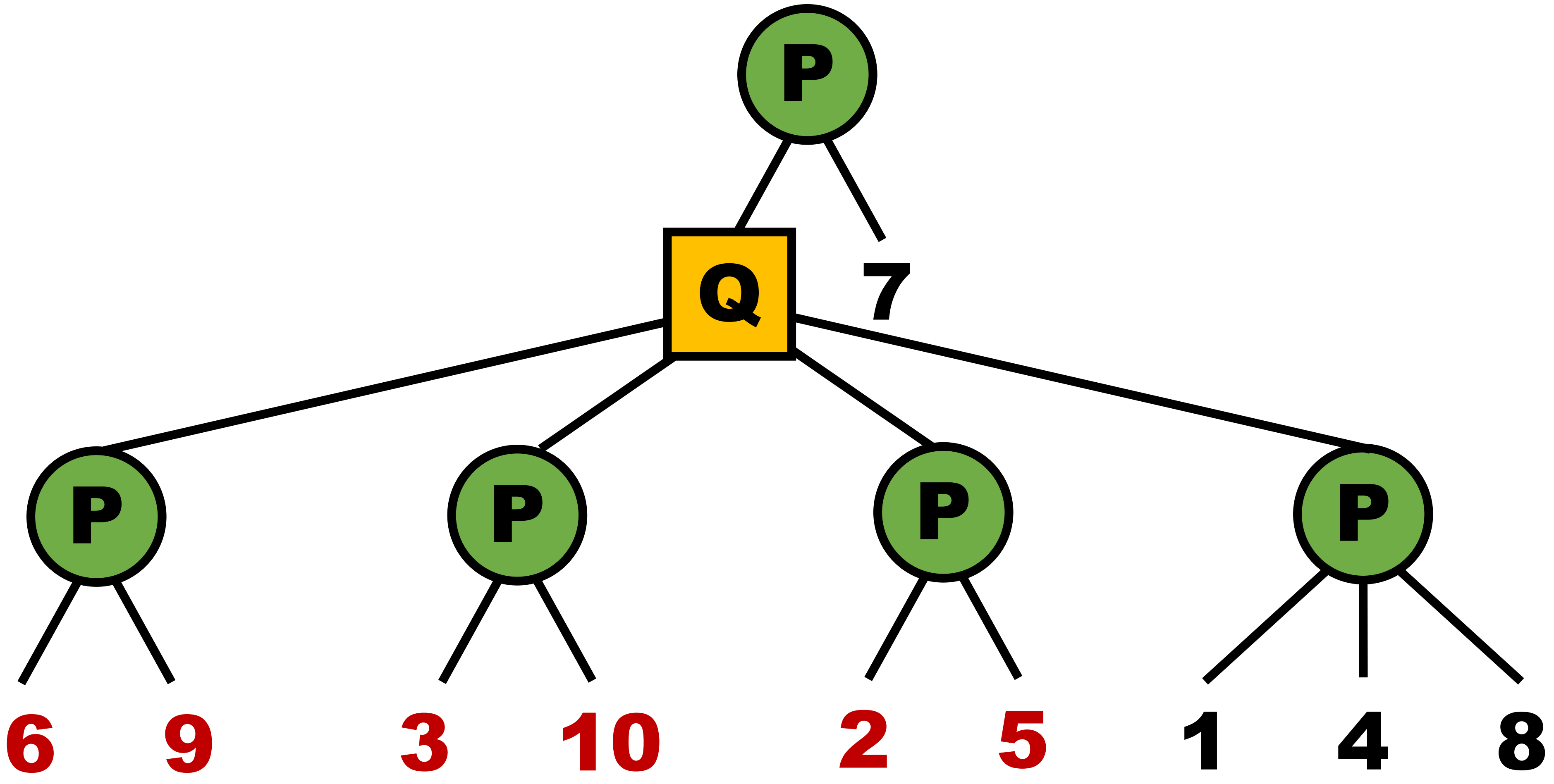


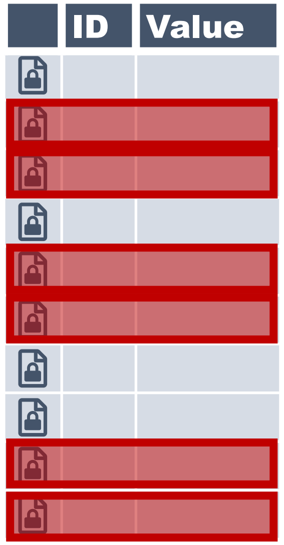
Query 3





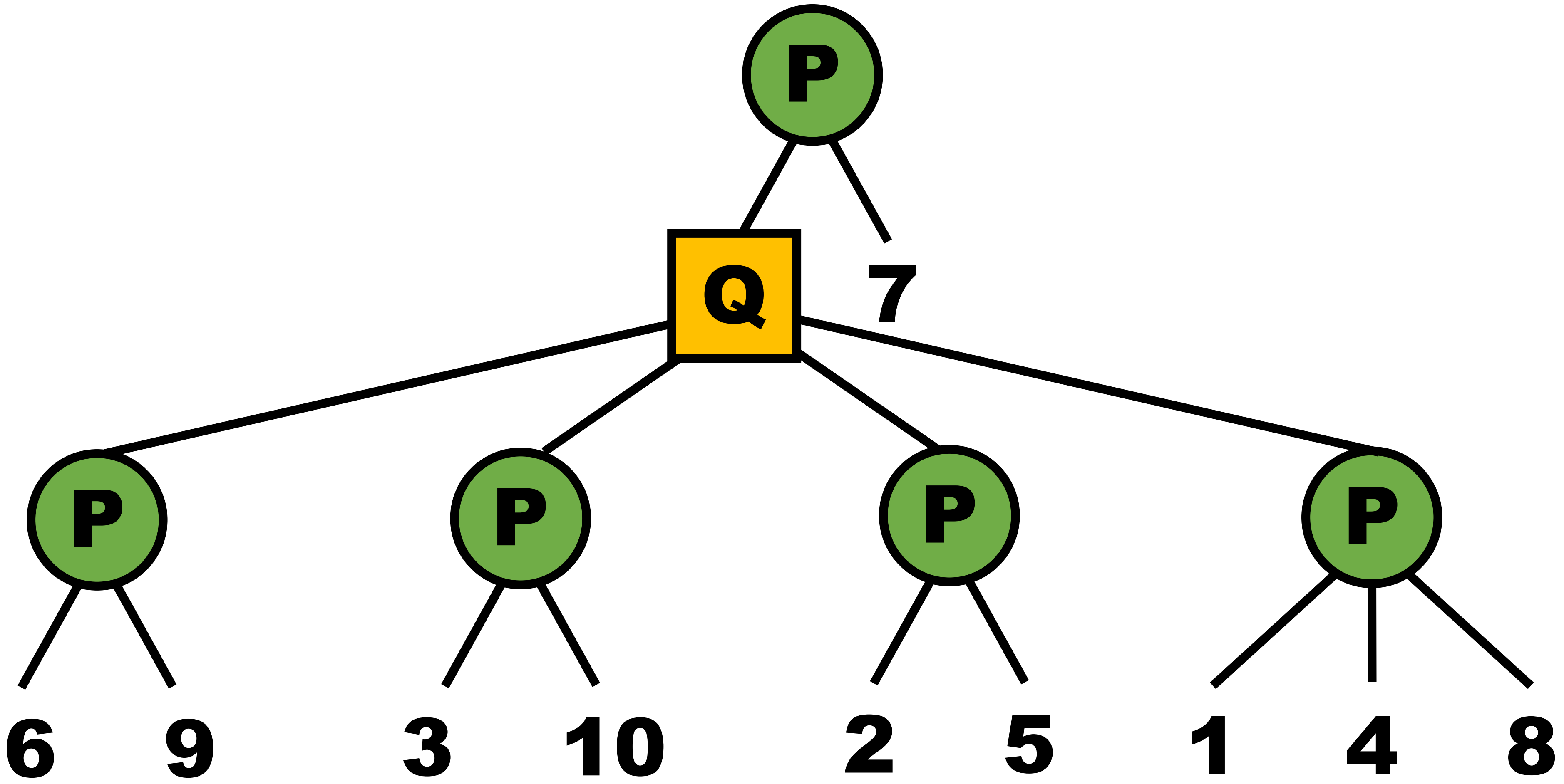
Query 3





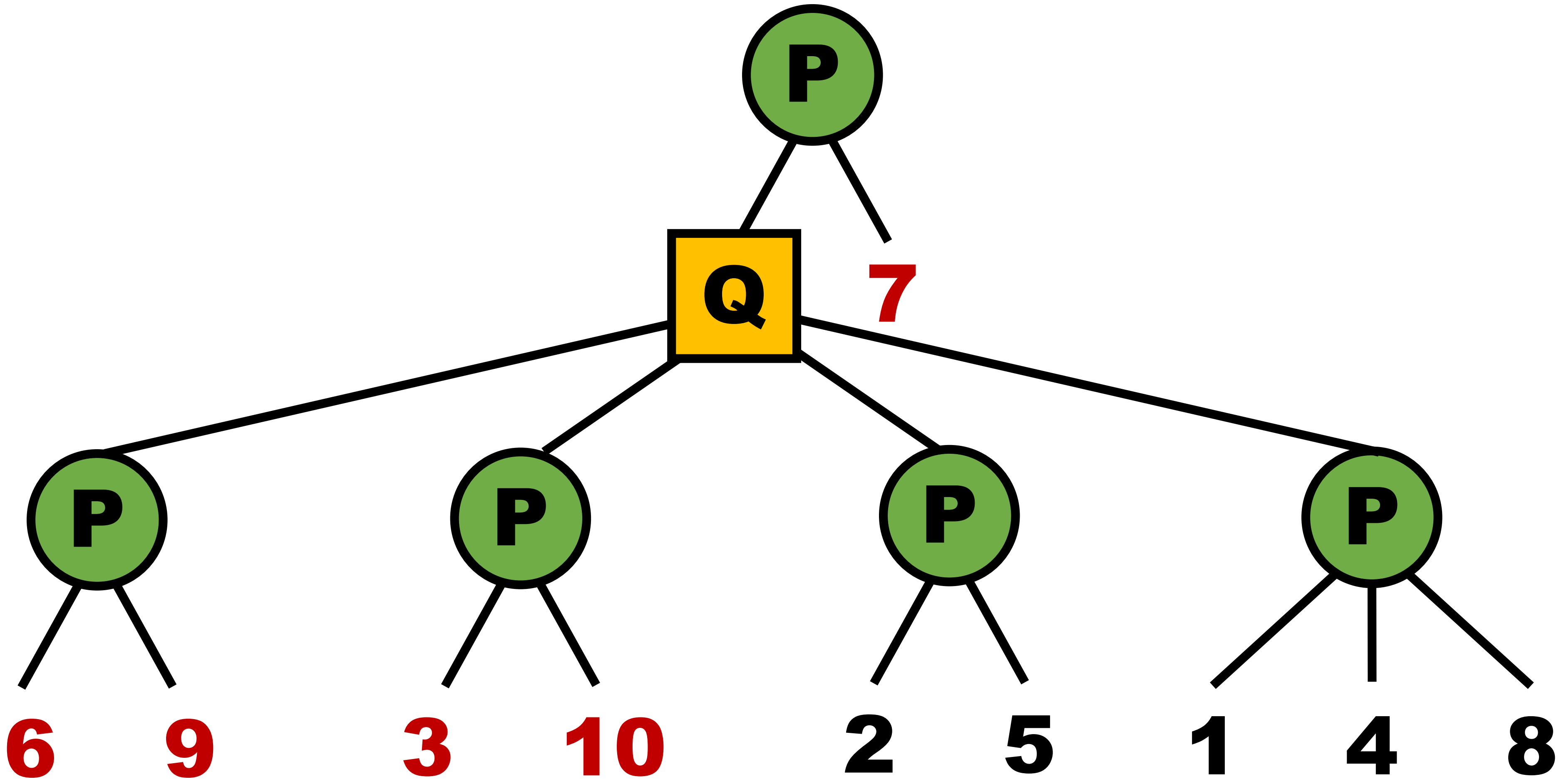
Query 3

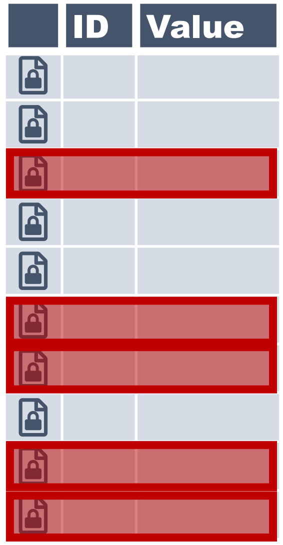
	ID	Value



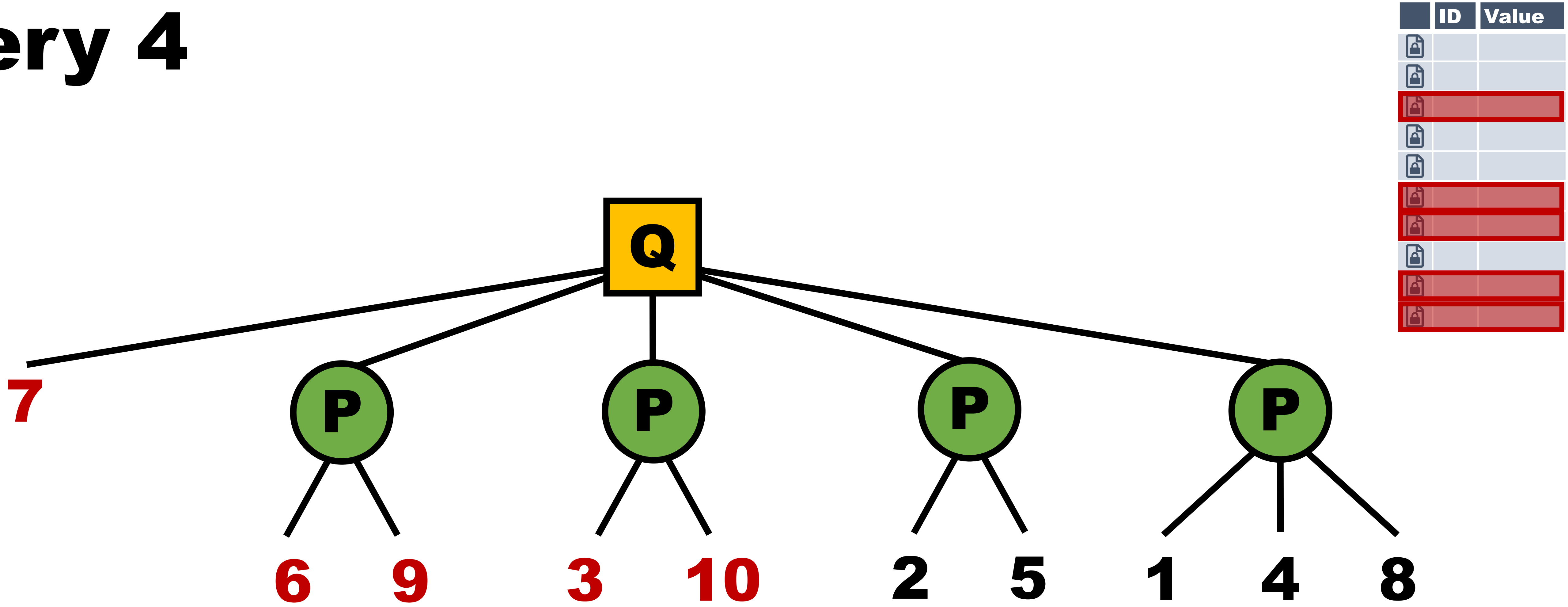
black hat USA 2019

Query 4

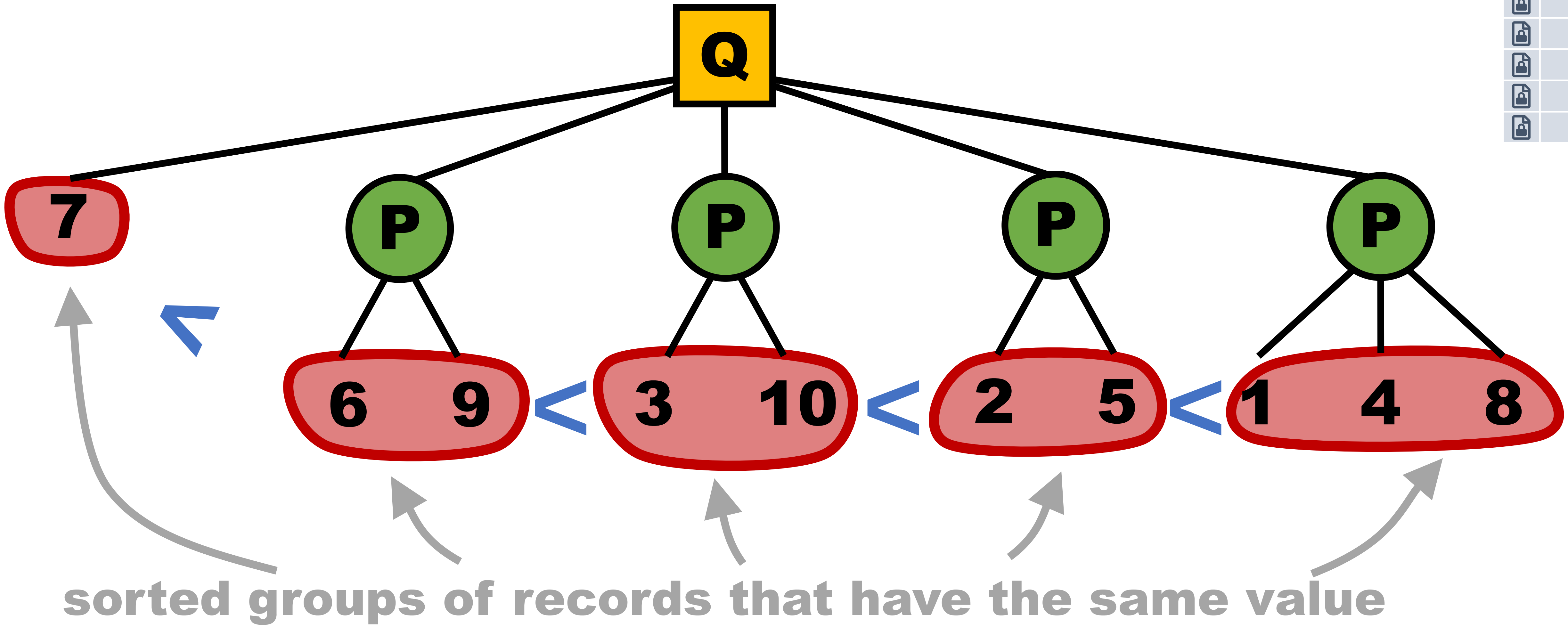




Query 4

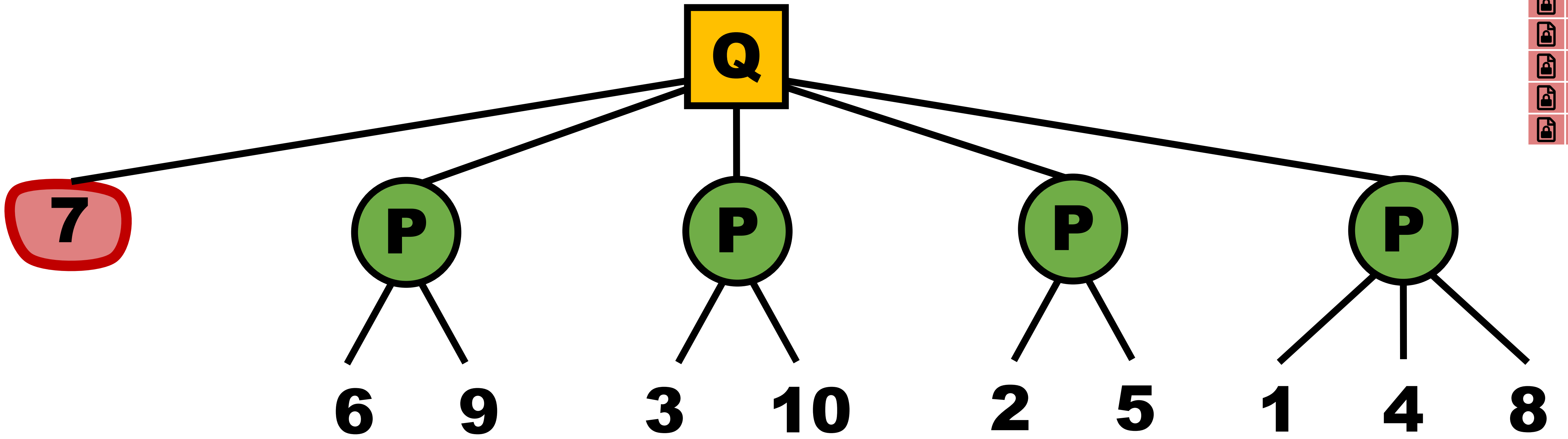


Fully Sorted and Grouped Records

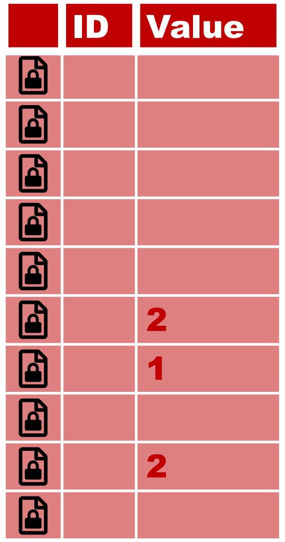


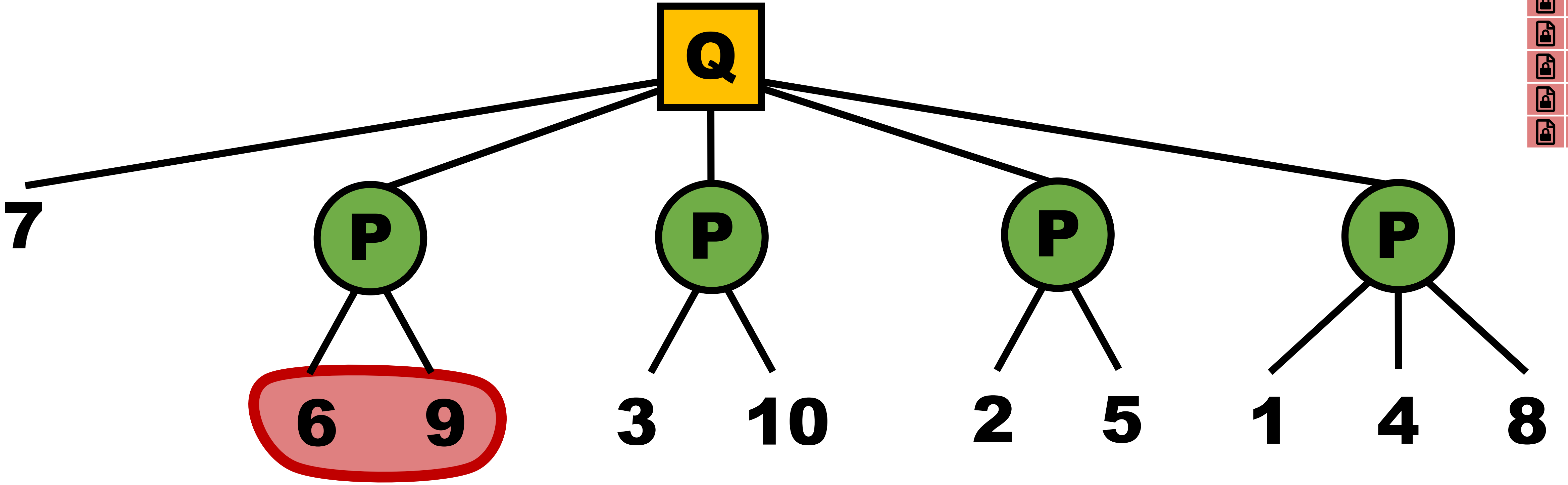
Fully Sorted and Grouped Records

	ID	Value
		1



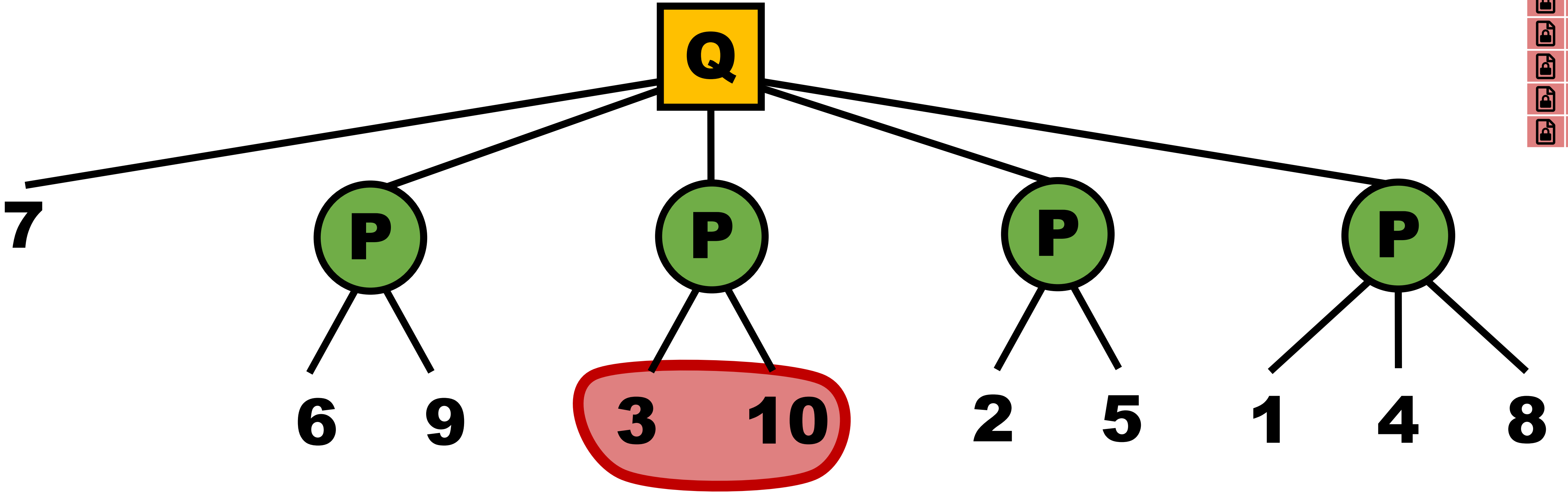
Fully Sorted and Grouped Records



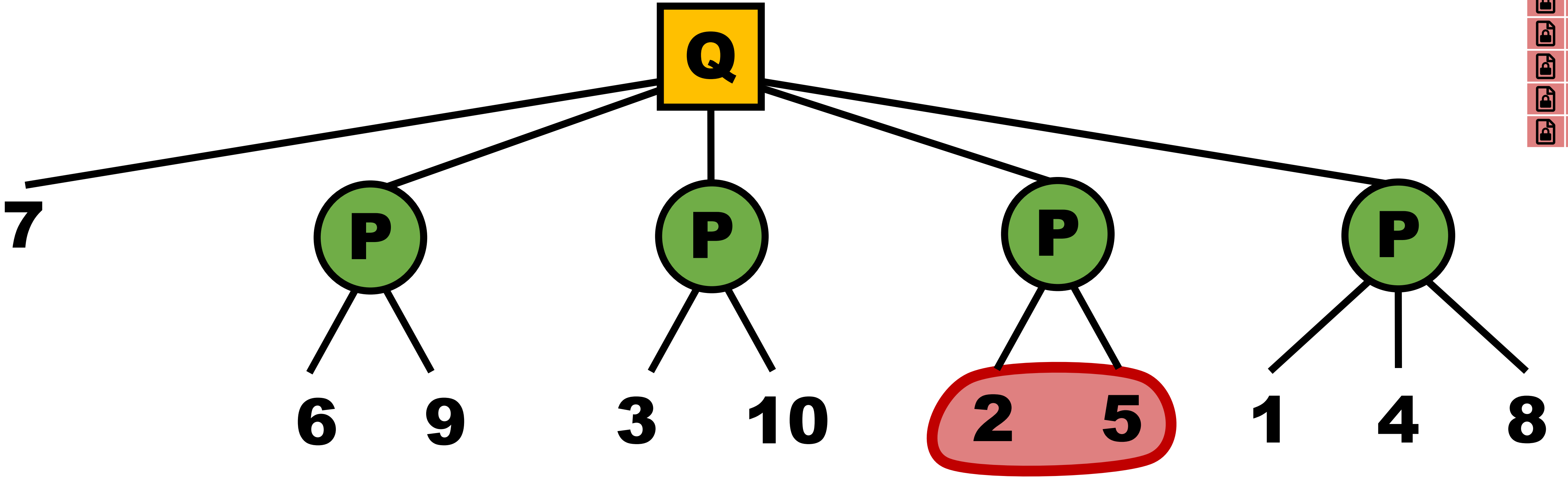


Fully Sorted and Grouped Records

	ID	Value
		3
		2
		1
		2
		3

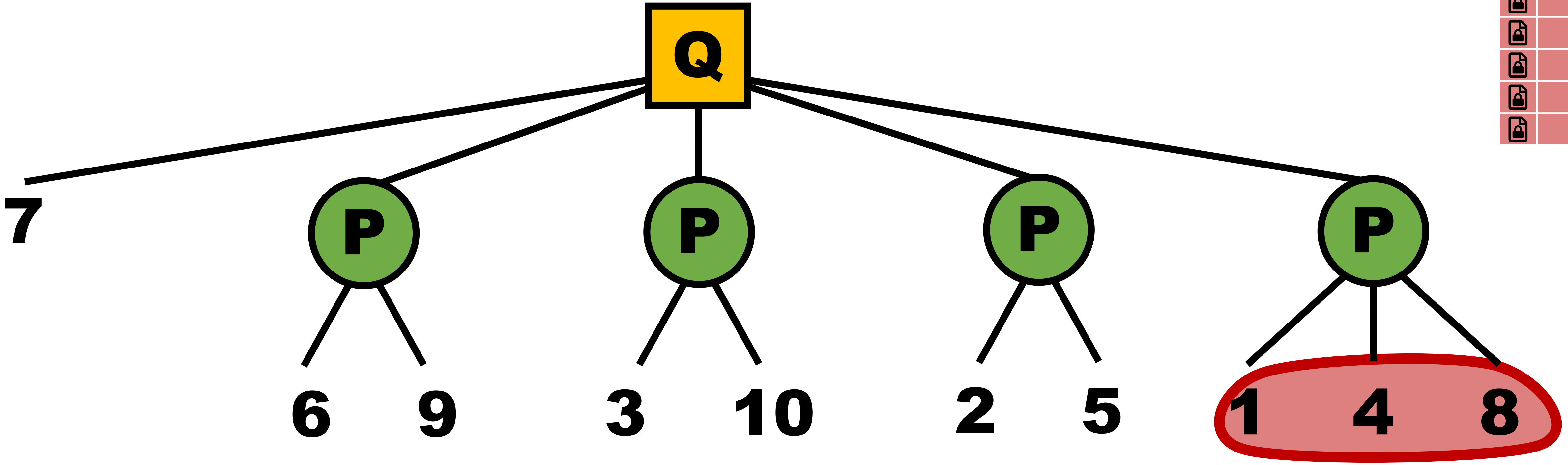


Fully Sorted and Grouped Records



	ID	Value
		4
		3
		4
		2
		1
		2
		3

Fully Sorted and Grouped Records



	ID	Value
		5
		4
		3
		5
		4
		2
		1
		5
		2
		3

Fully Sorted and Grouped Records

	ID	Value
	1	**5**
	2	**4**
	3	**3**
	4	**5**
	5	**4**
	6	**2**
	7	**1**
	8	**5**
	9	**2**
	10	**3**

How Many Queries Are Needed?

Suppose values are in {1, …, N}.

EXACT RECONSTRUCTION

How Many Queries Are Needed?

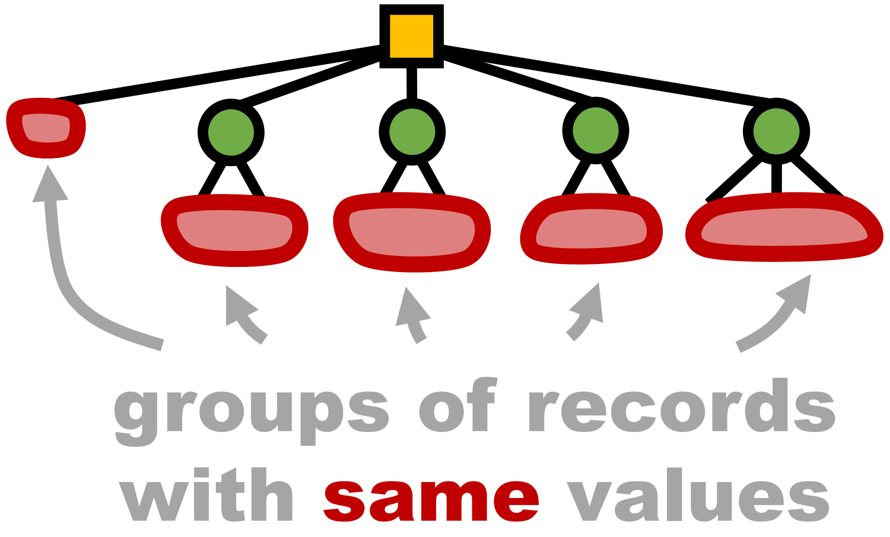
Suppose values are in {1, …, N}.

EXACT RECONSTRUCTION

N log N queries

e.g.,

N=10: **23**, N=100: **461**, N=1000: **6908**

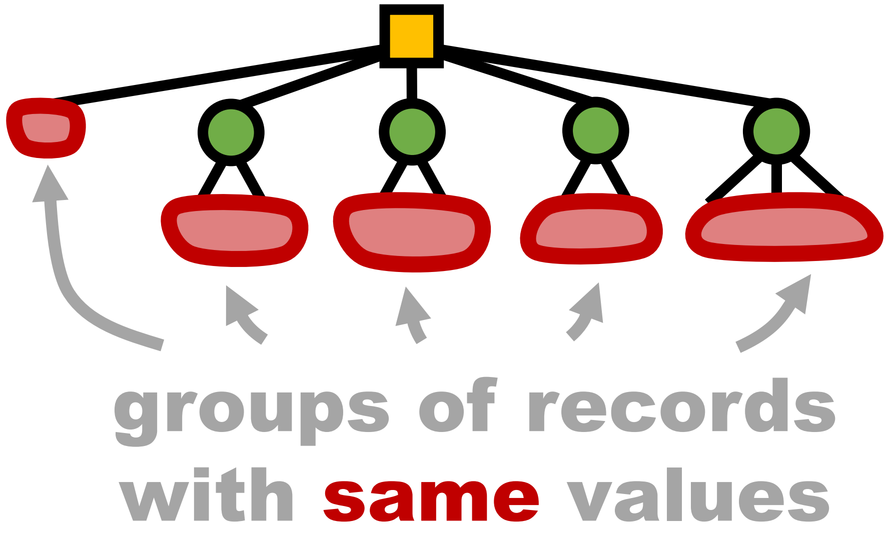


How Many Queries Are Needed?

Suppose values are in {1, …, N}.

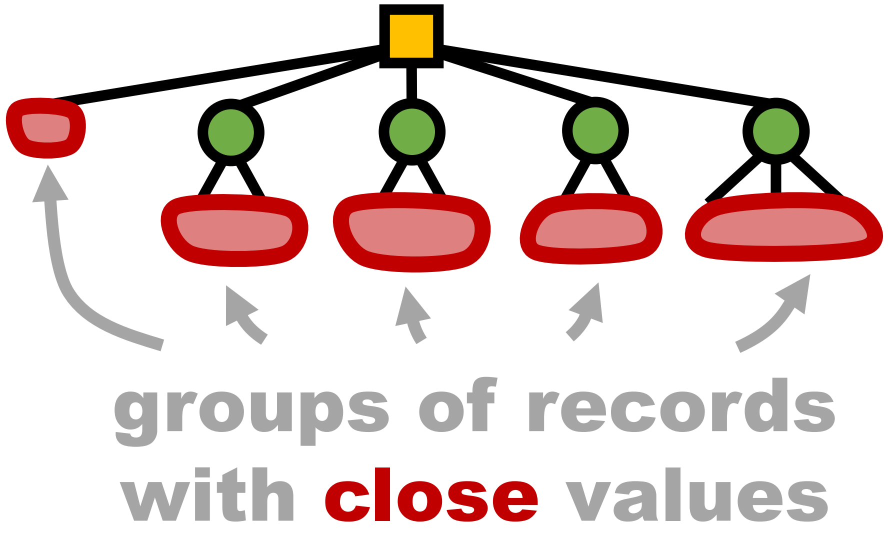
EXACT RECONSTRUCTION

N log N queries
e.g.,
N=10: **23**, N=100: **461**, N=1000: **6908**



APPROXIMATE RECONSTRUCTION

Depends only on precision
(values within some % of N)
e.g., 10%: **23**, 5%: **60**, 2%: **460**

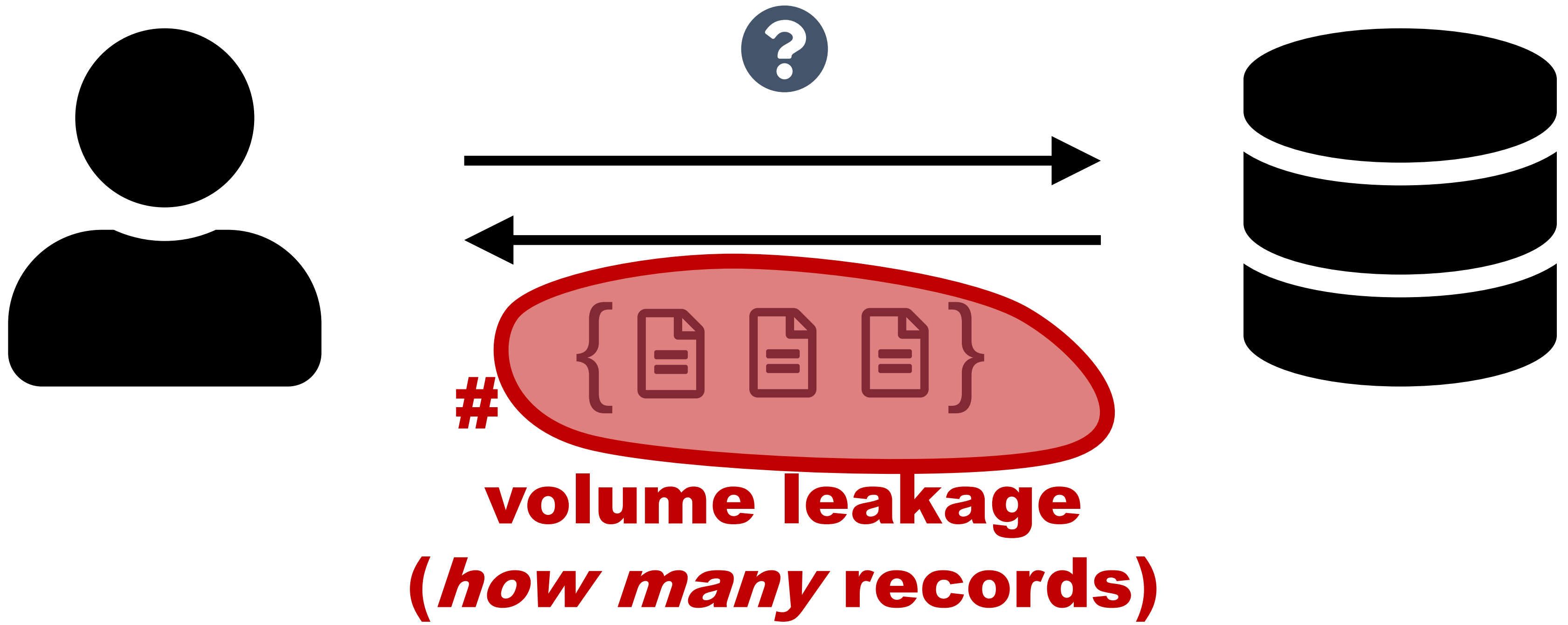


Exploiting Access Pattern Leakage

- Leaking **which rows** match a query can break encryption.
- **PQ trees** help organize the leakage along the way.
- Recovering **approximate** values takes even fewer queries.

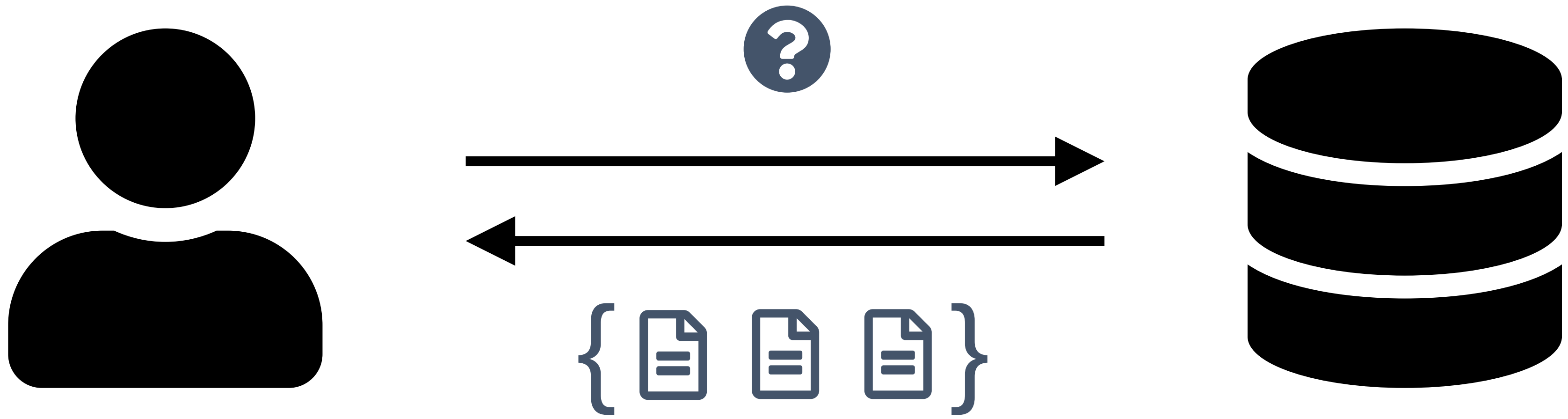
Details: [Grubbs, Lacharité, Minaud, and Paterson, S&P 2019]

Exploiting Volume Leakage



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Exploiting Volume Leakage

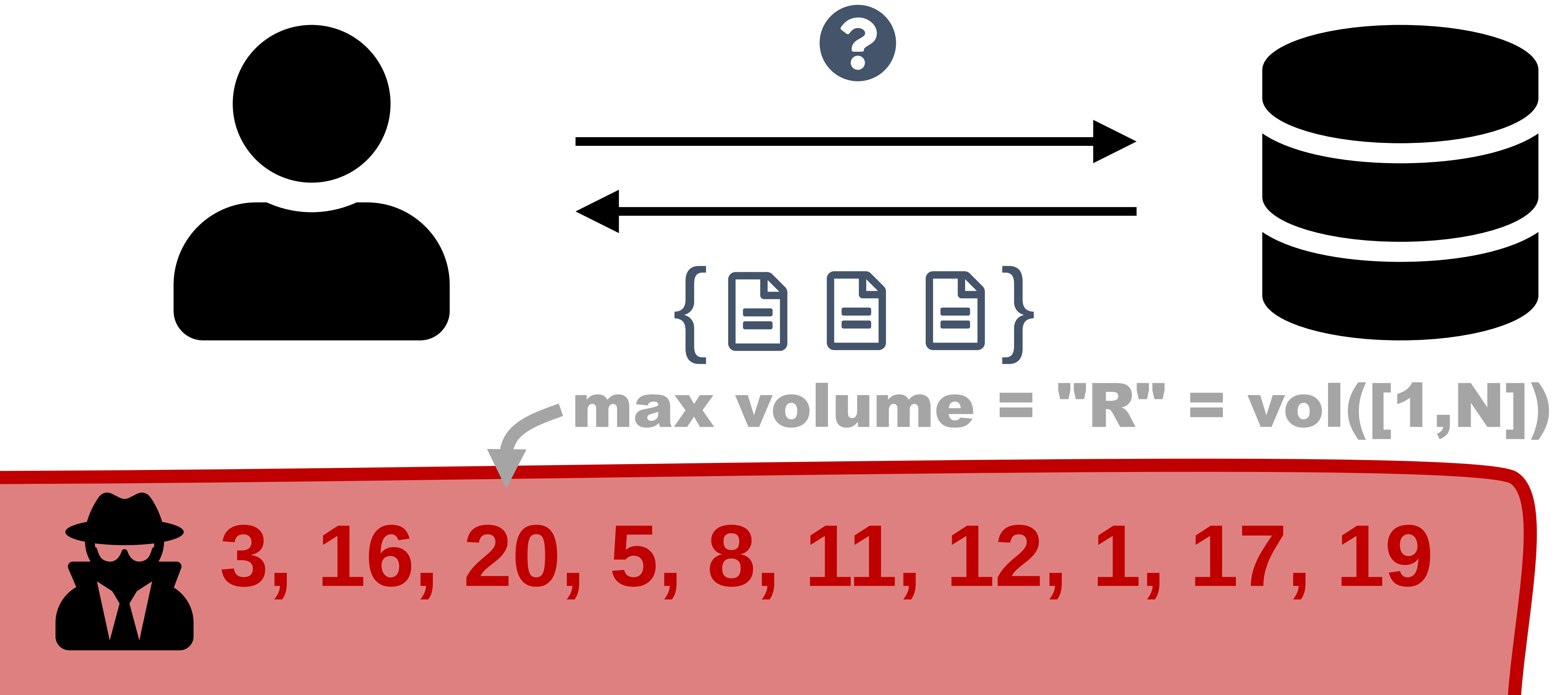


	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

3, 16, 20, 5, 8, 11, 12, 1, 17, 19

all possible range volumes

Exploiting Volume Leakage

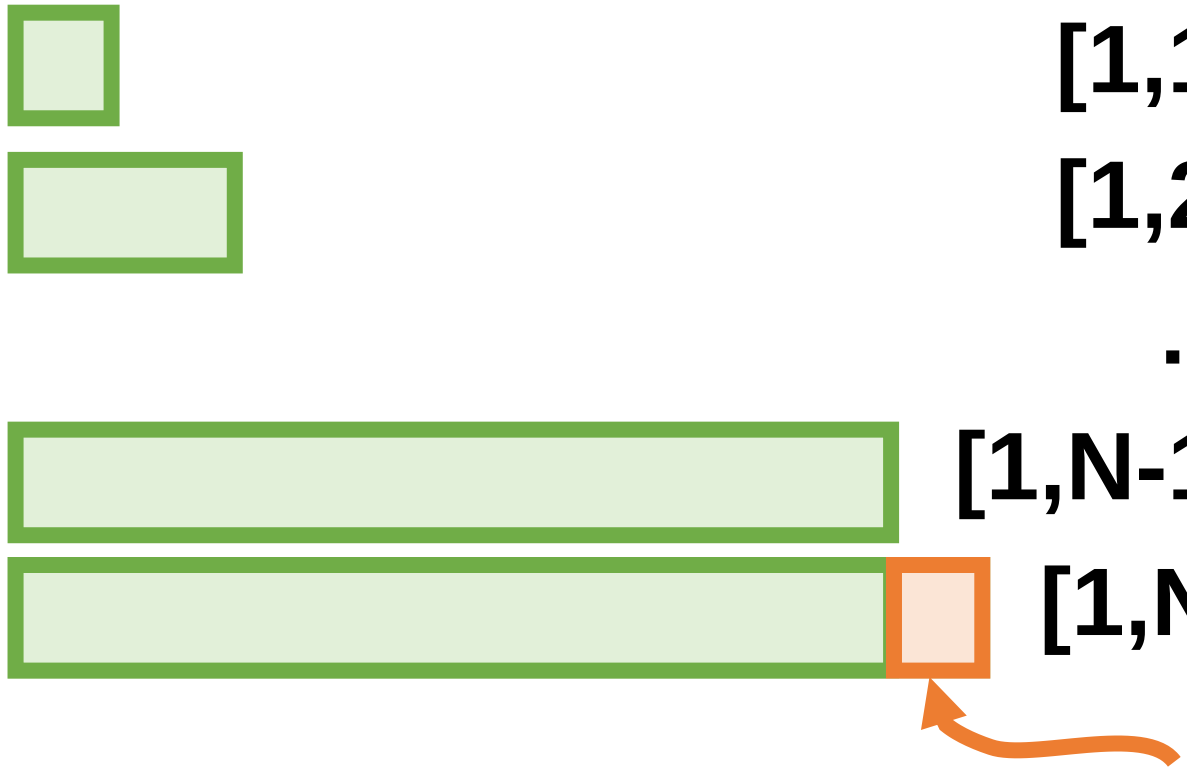


	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

The Idea: Identify Elementary Volumes

ELEMENTARY RANGES	ELEMENTARY VOLUMES
[1,1]	# rows matching [1,1],
[1,2]	# rows matching [1,2],
…	…
[1,N-1]	# rows matching [1,N-1]
[1,N]	# rows matching [1,N]

The Idea: Identify Elementary Volumes



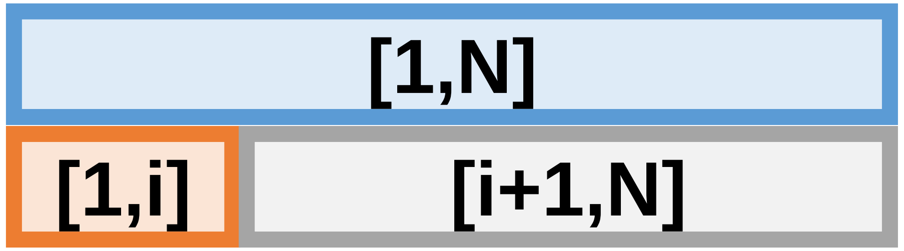
ELEMENTARY RANGES	ELEMENTARY VOLUMES
[1,1]	# rows matching [1,1],
[1,2]	# rows matching [1,2],
...	...
[1,N-1]	# rows matching [1,N-1]
[1,N]	# rows matching [1,N]

vol([1,N]) – vol([1,N-1]) = vol([N,N])

Elementary Properties

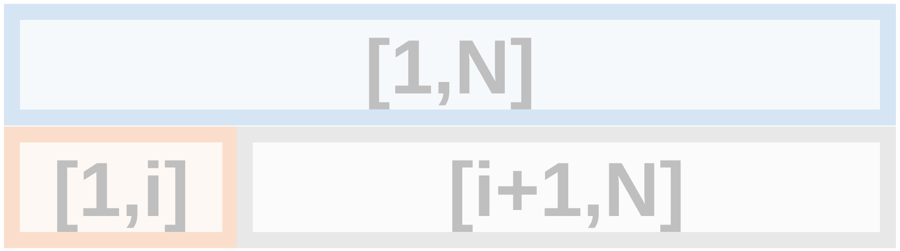
1. Such volumes are **R**-complemented:

   vol([1,i]) + vol([i+1,N]) = R

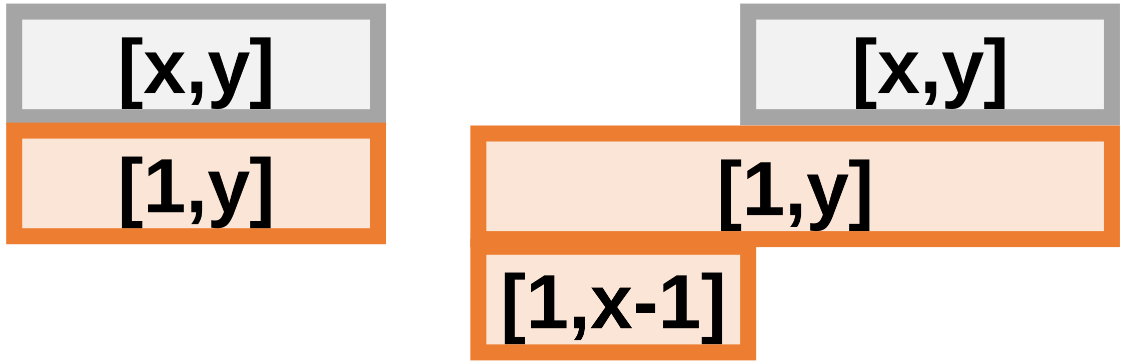


Elementary Properties

1. Such volumes are **R**-complemented:
   vol([1,i]) + vol([i+1,N]) = R

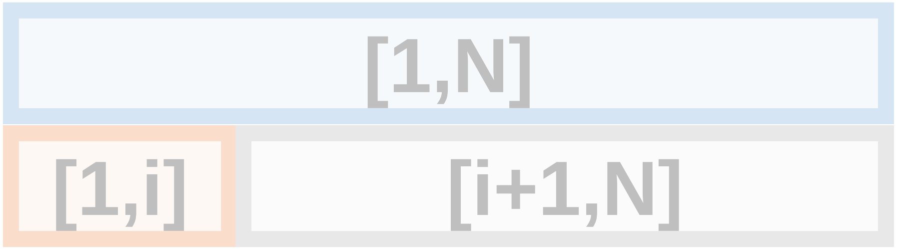


2. Every range [x,y] has the form
   [1,y] **or** [1,y] \ [1,x-1]

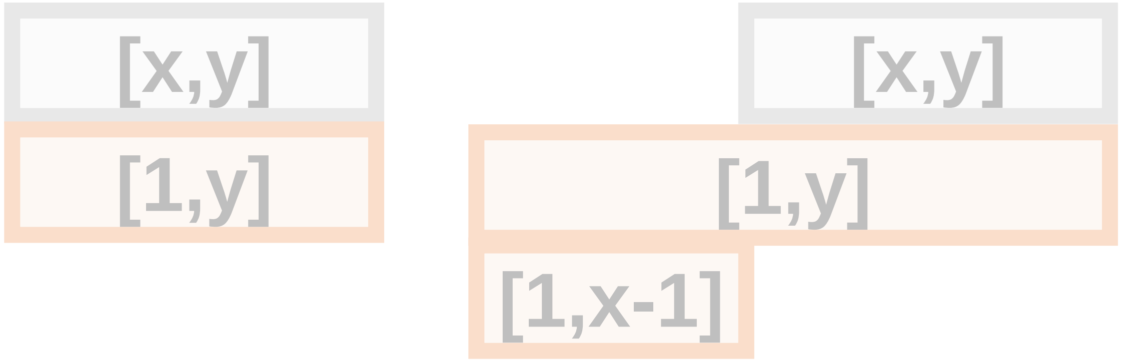


Elementary Properties

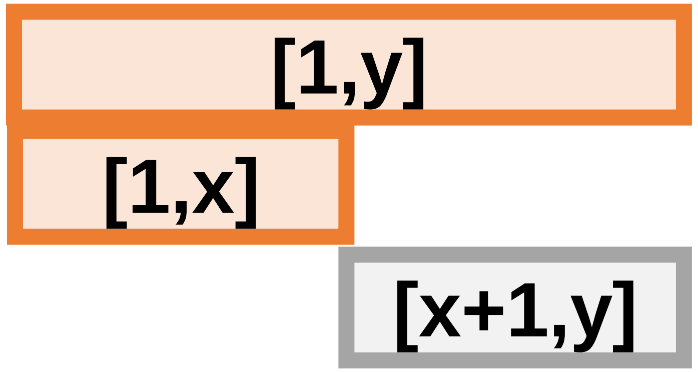
1. Such volumes are **R**-complemented:
   vol([1,i]) + vol([i+1,N]) = R



2. Every range [x,y] has the form
   [1,y] **or** [1,y] \ [1,x-1]



3. Difference of any two such ranges is a range:
   [1,y] \ [1,x] = [x+1,y]



Let's Build a Graph

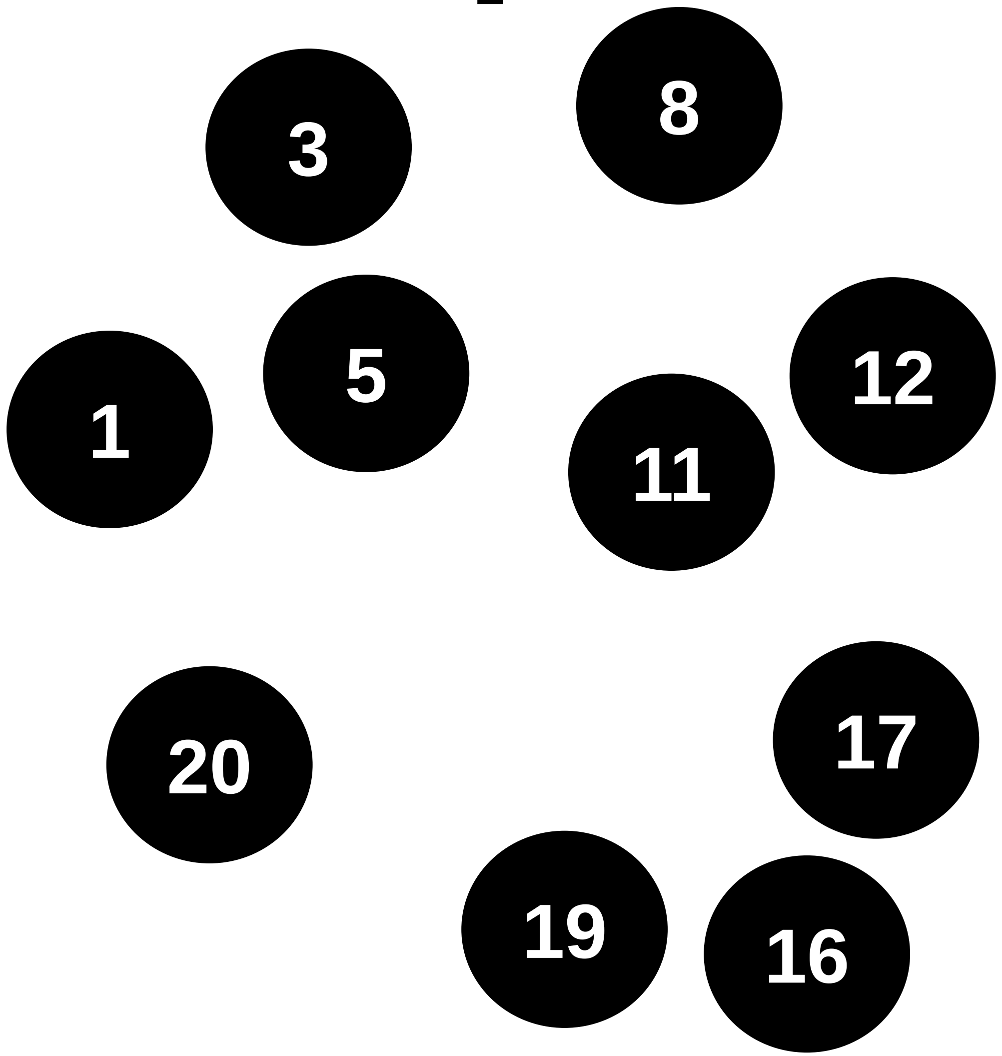
set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

Let's Build a Graph

Nodes = observed volumes

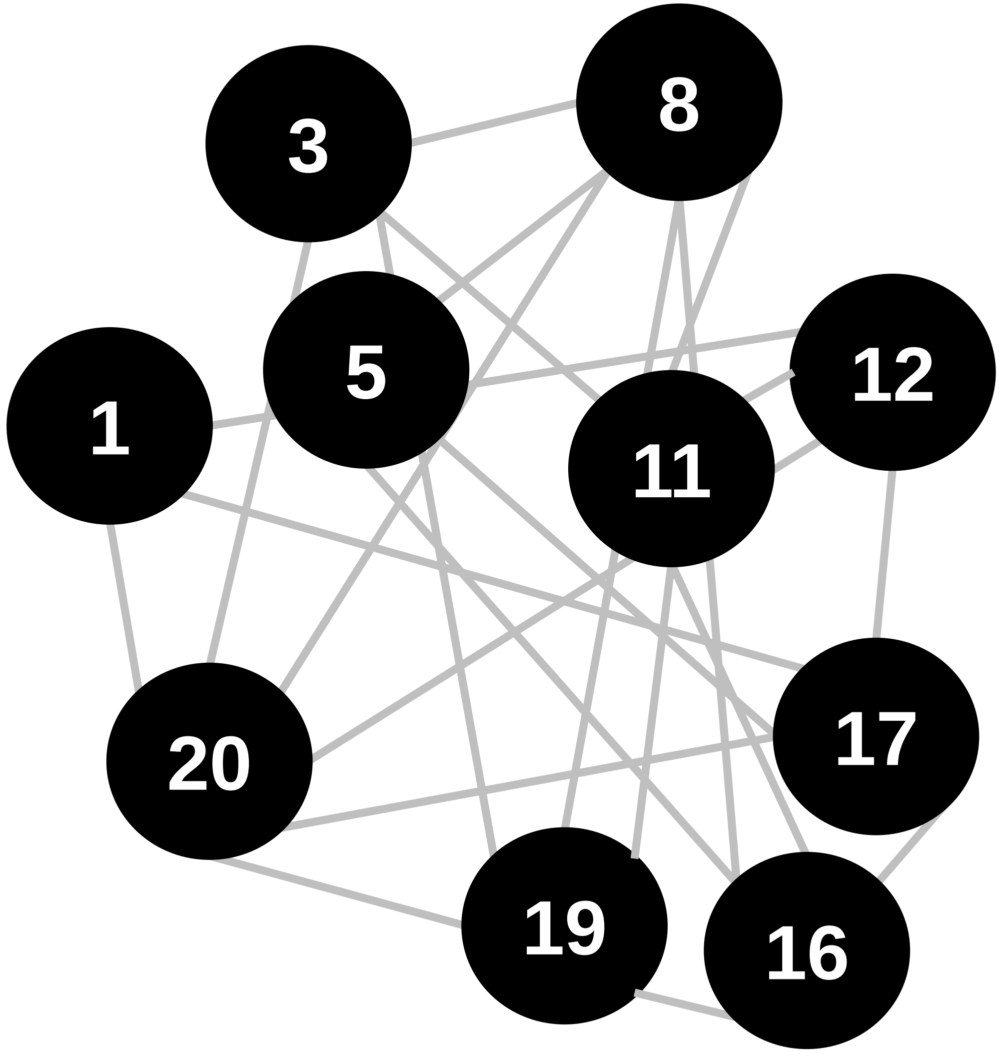
set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

Let's Build a Graph



Nodes = observed volumes

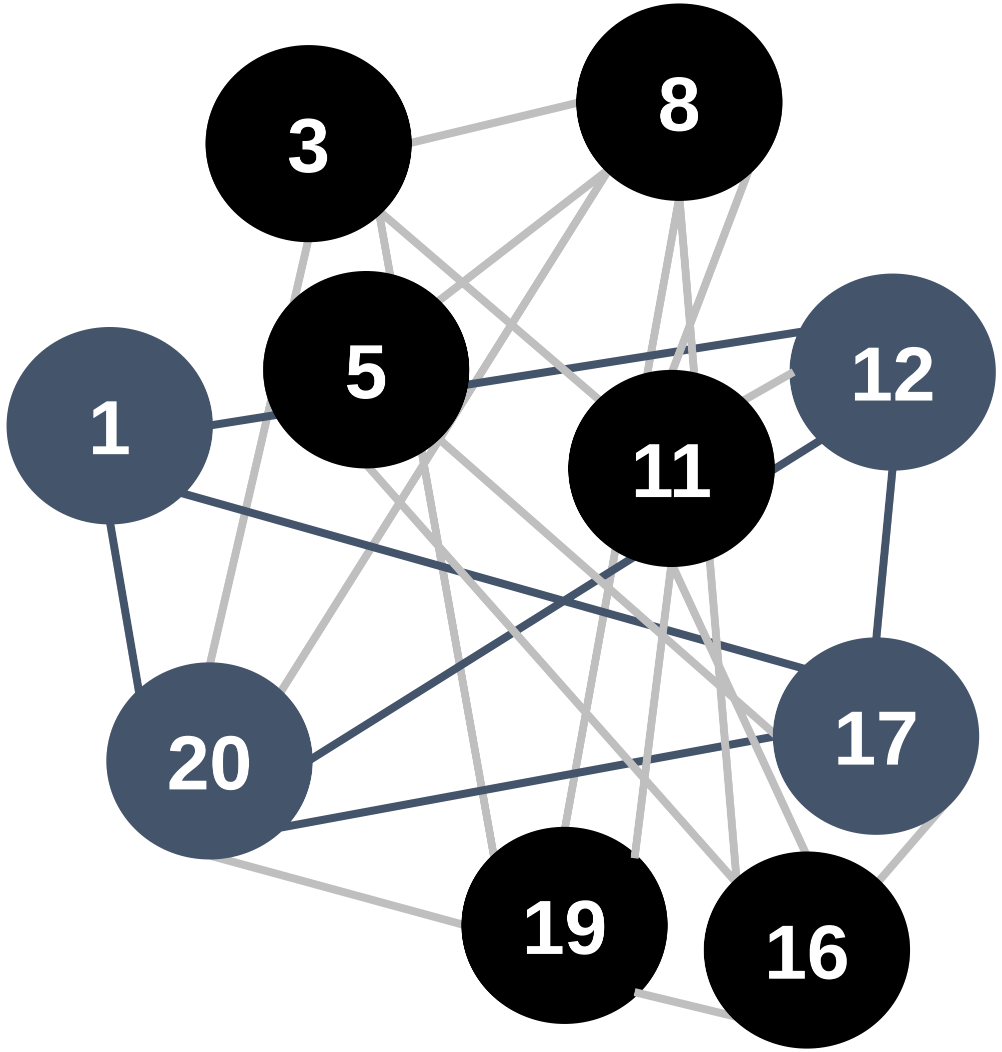
set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20



Edge iff difference was also a volume

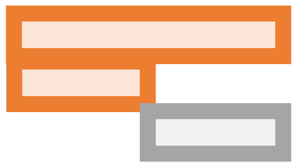
set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

Elementary volumes form a clique



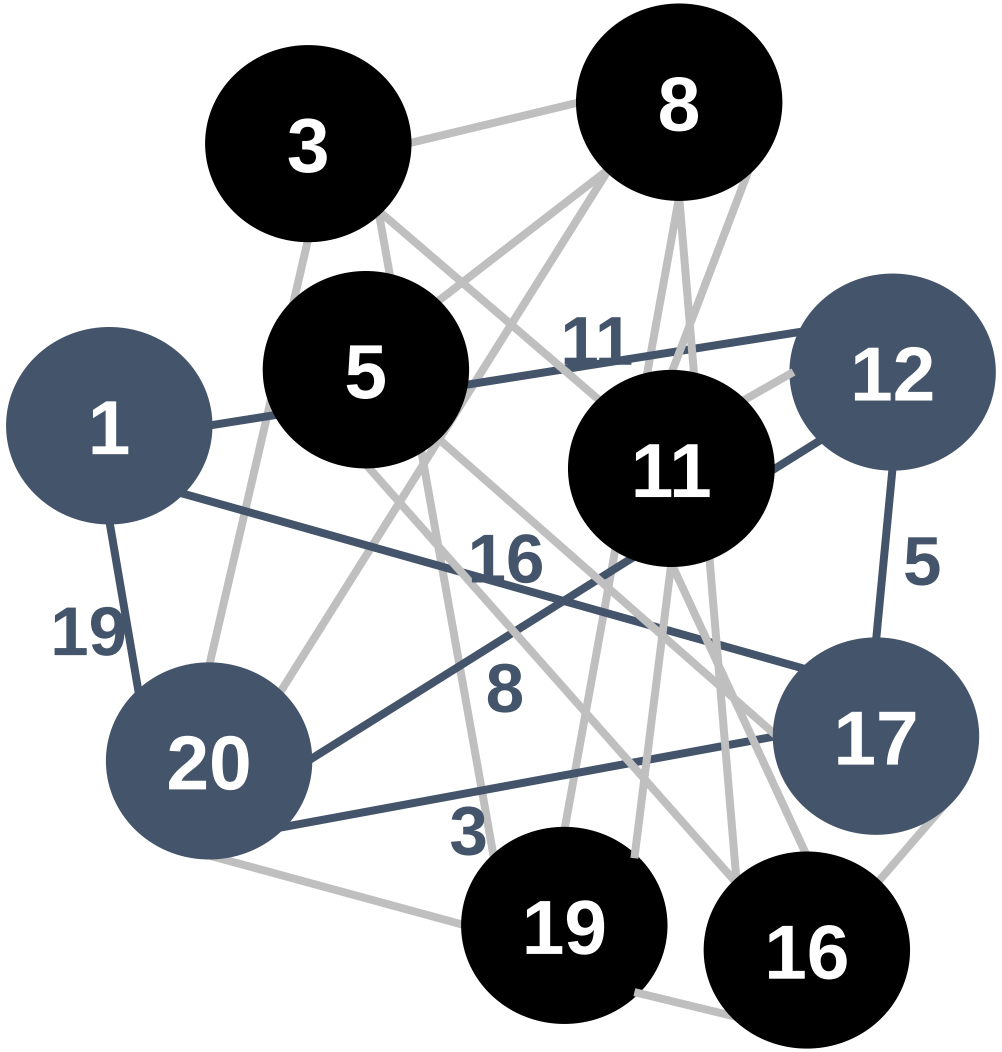
Property 3:

[1,y] \ [1,x] = [x+1,y]



set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

Elementary volumes form a clique… that generates all volumes



Property 2:

[x,y] has the form [1,y] or [1,y] \ [1,x-1]

set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

Exploiting Volume Leakage

Goal: identify set of elementary volumes

Idea: build a graph and find a clique in it

Exploiting Volume Leakage

Goal: identify set of elementary volumes

Idea: build a graph and find a clique in it

Phases:

1. Pre-processing
2. "Traditional" clique-finding

usually not necessary, see my paper for details

Phase 1: Pre-Processing

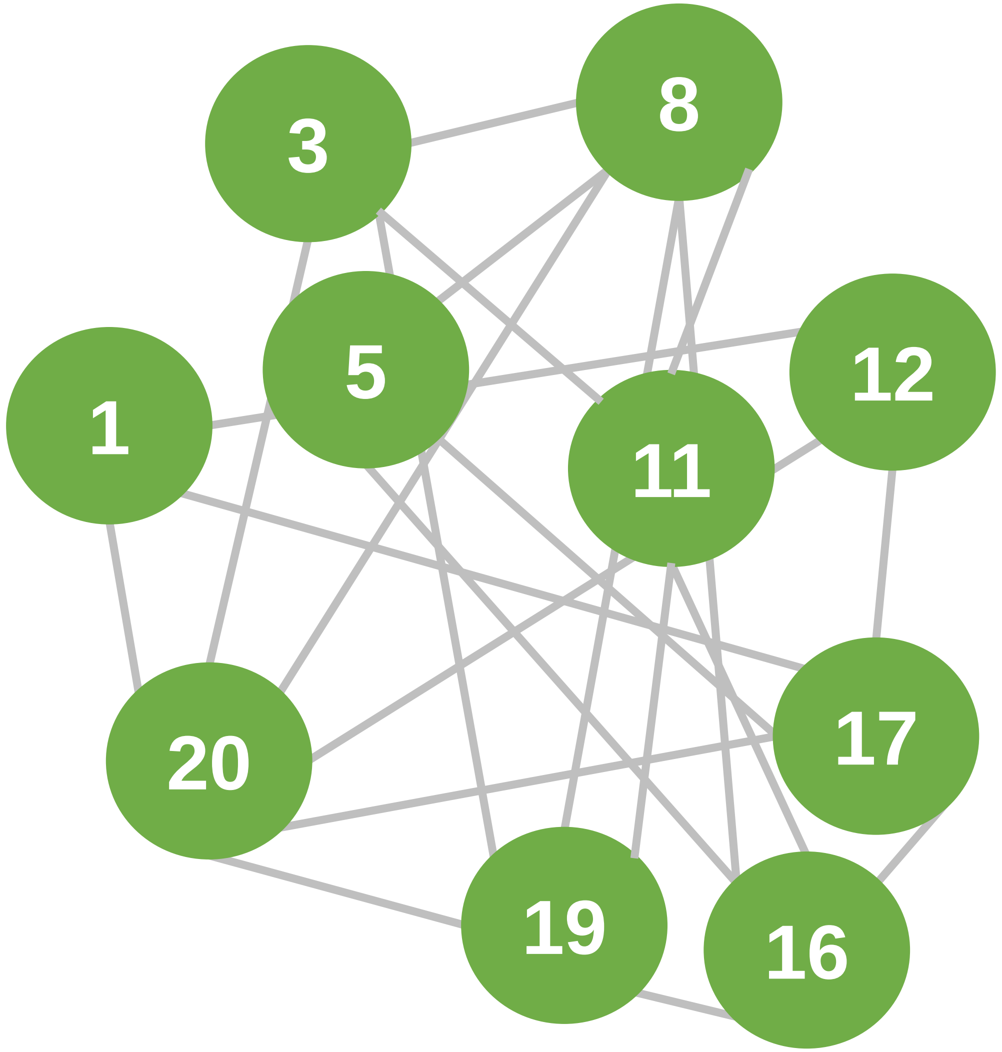
NECESSARY ELEMENTARY VOLUMES	$\subseteq$	REAL ELEMENTARY VOLUMES	$\subseteq$	CANDIDATE ELEMENTARY VOLUMES

Phase 1: Pre-Processing

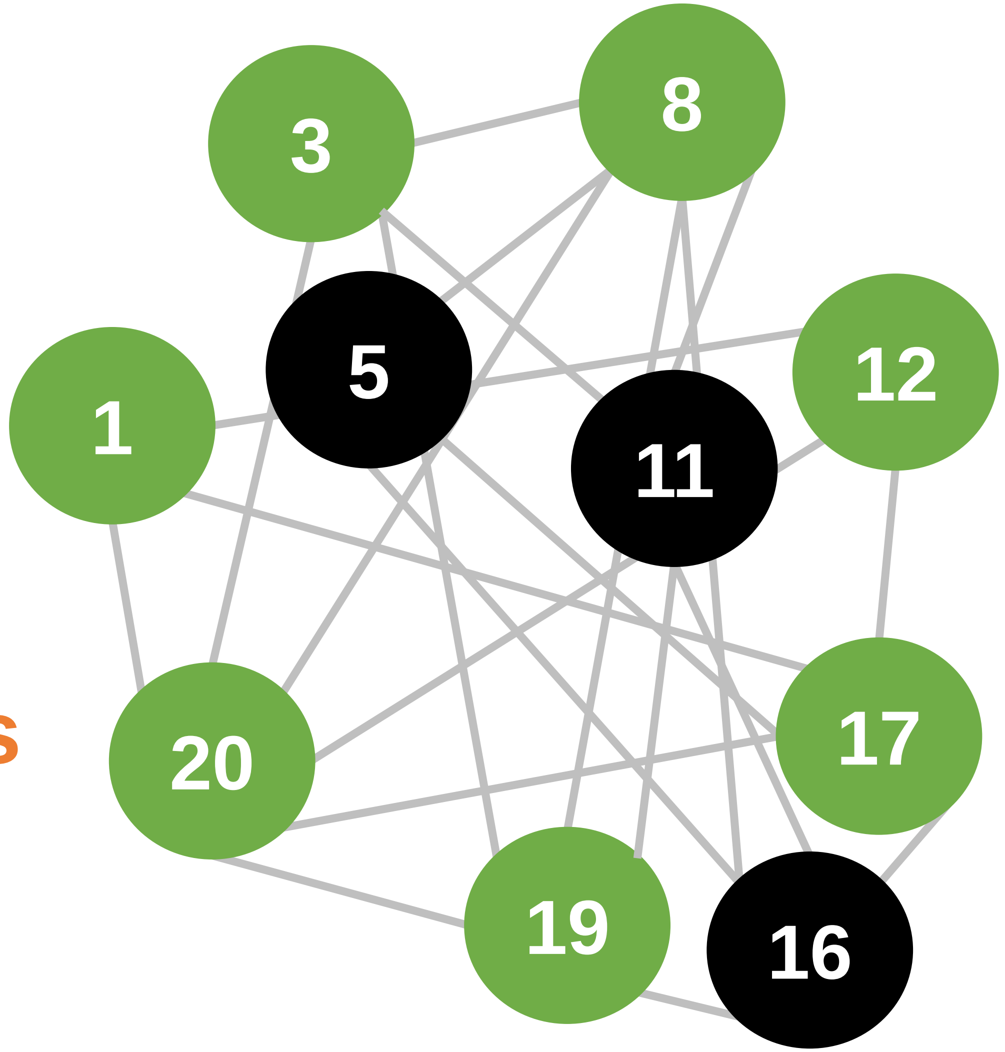
NECESSARY ELEMENTARY VOLUMES $\subseteq$ REAL ELEMENTARY VOLUMES $\subseteq$ CANDIDATE ELEMENTARY VOLUMES

AUGMENT NECESSARY VOLUMES $\longleftrightarrow$ REDUCE CANDIDATE VOLUMES

Example



set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

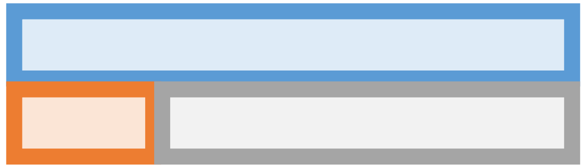


REDUCE

Remove nodes without *R*-complements

Property 1:

Elementary volumes are R-complemented

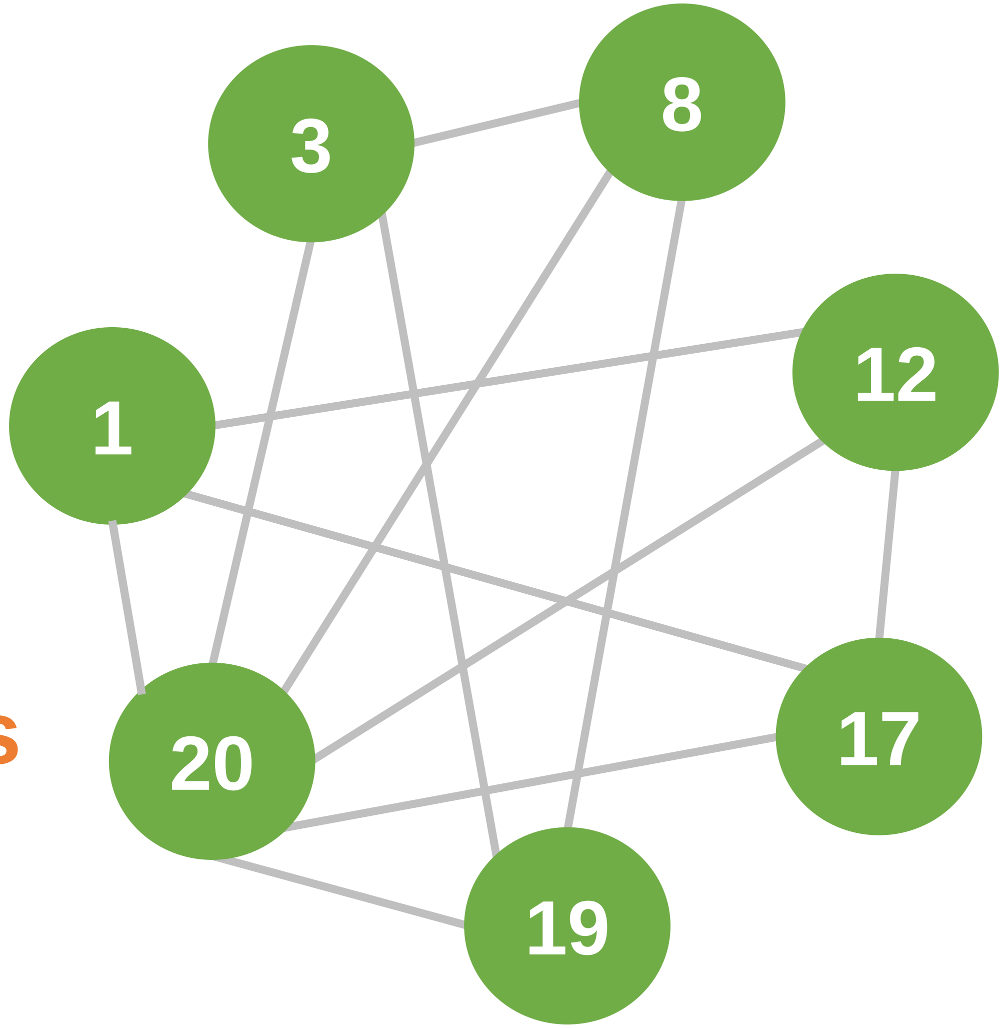


set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

REDUCE

Property 1:

Elementary volumes are R-complemented



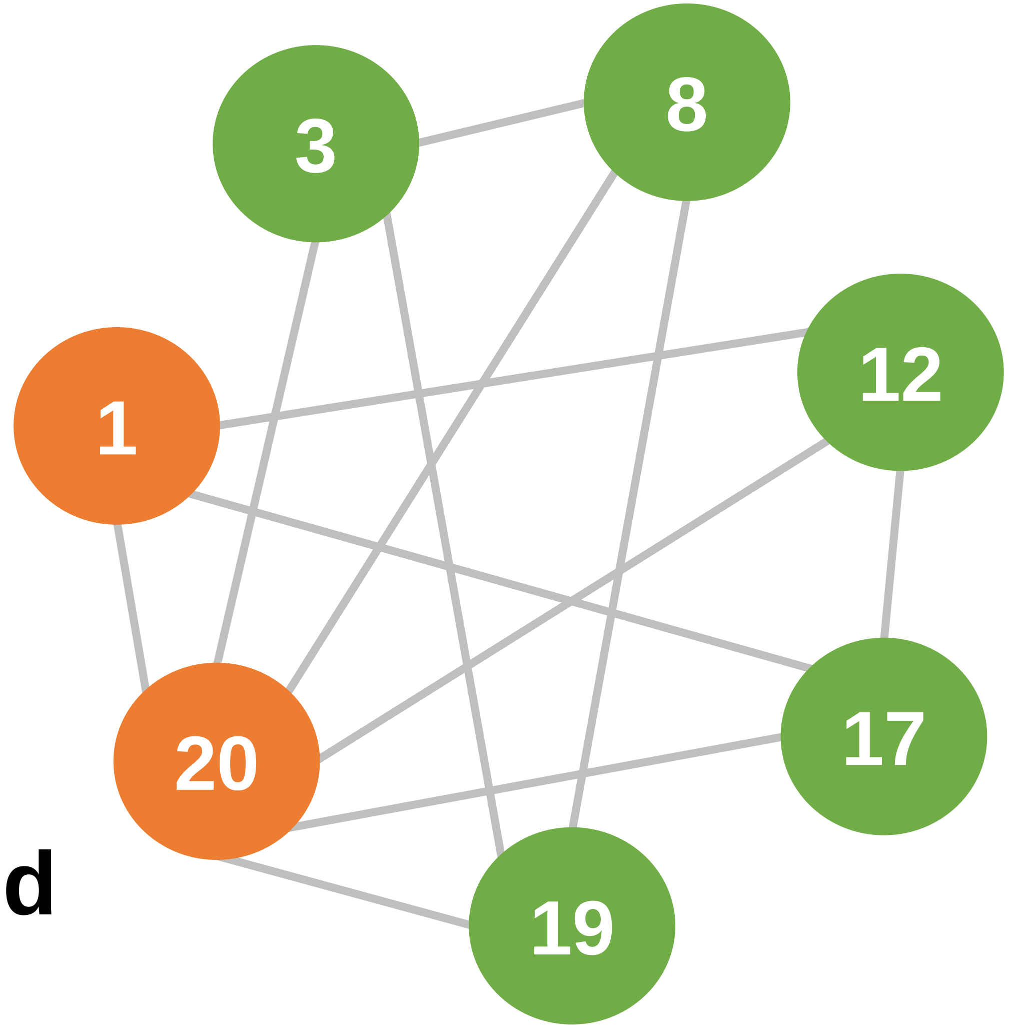
Remove nodes without *R*-complements

set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

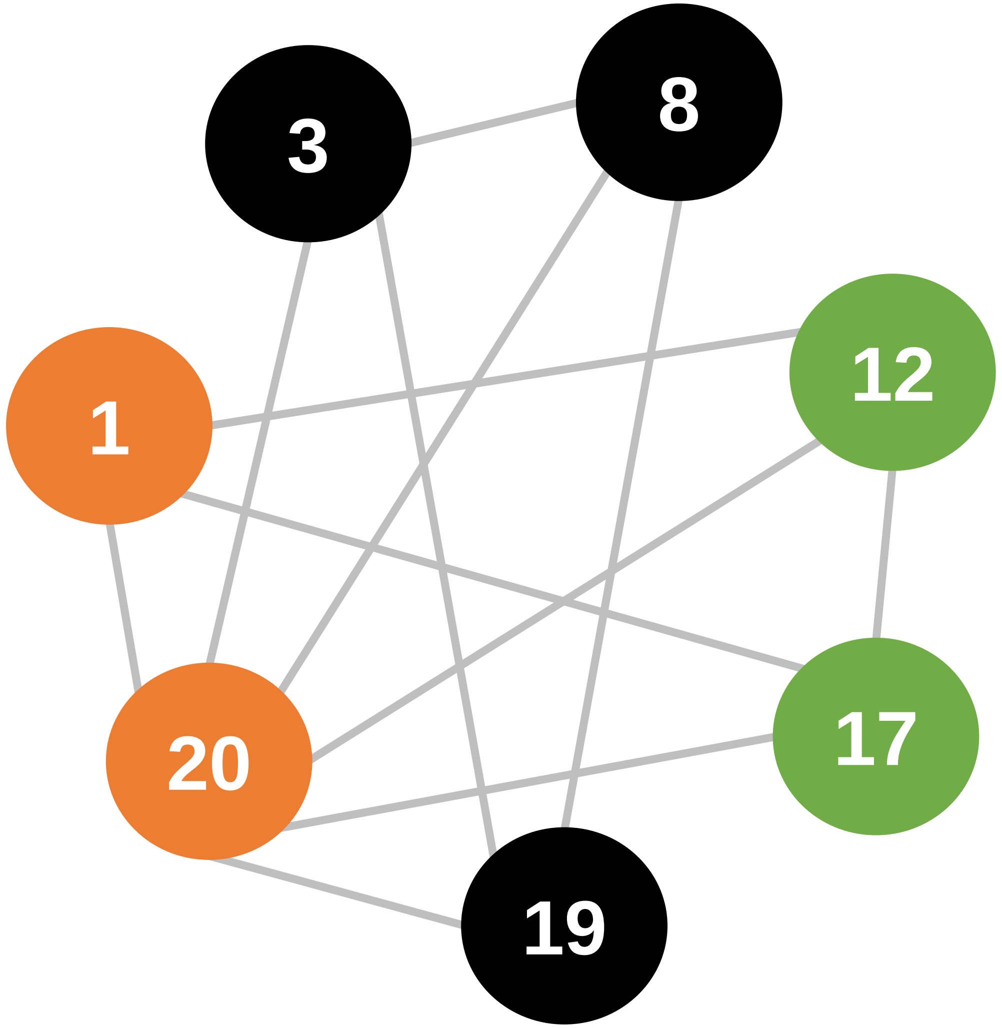
AUGMENT

Smallest complemented volume

Largest complemented volume (R)



set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20



REDUCE

Remove nodes not adjacent to all necessary volumes

set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

REDUCE

Remove nodes not adjacent to all necessary volumes

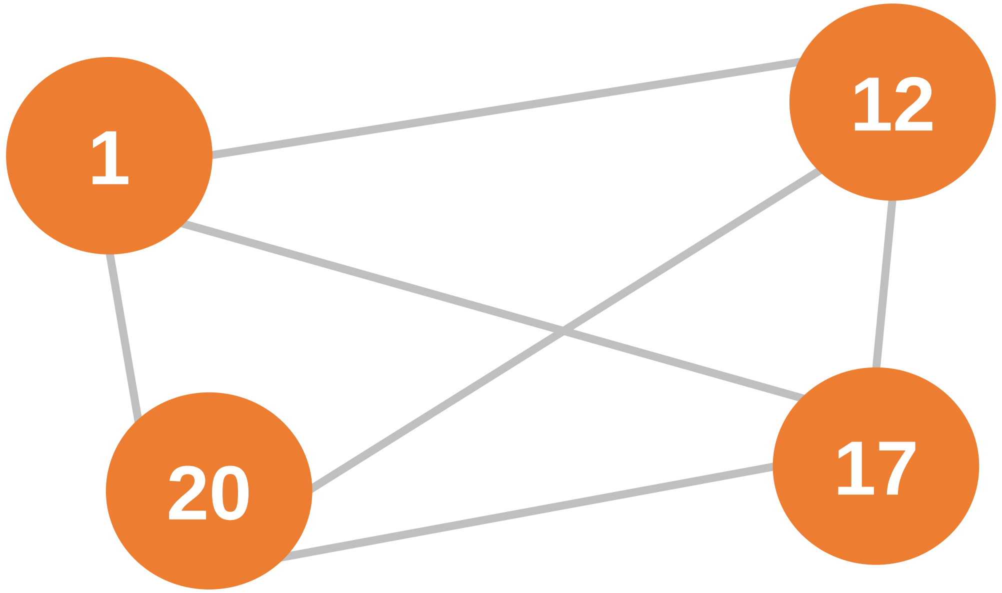
set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

AUGMENT

Add endpoints of volumes that occur only once, as an edge

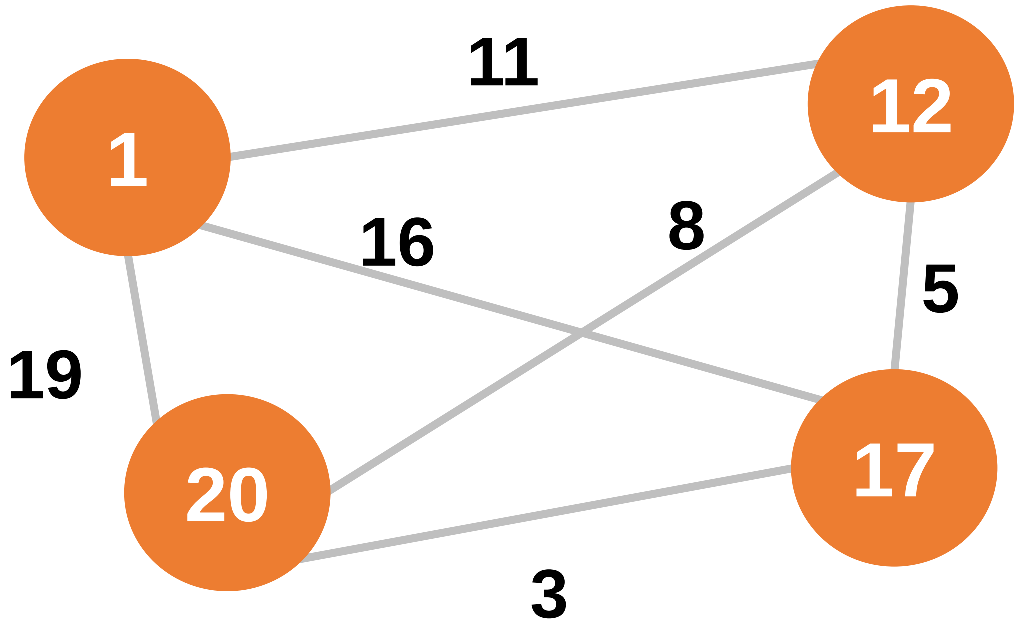
set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

AUGMENT



Add endpoints of volumes that occur only once, as an edge

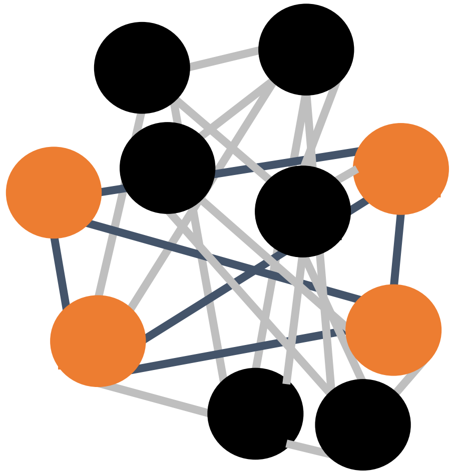
set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20



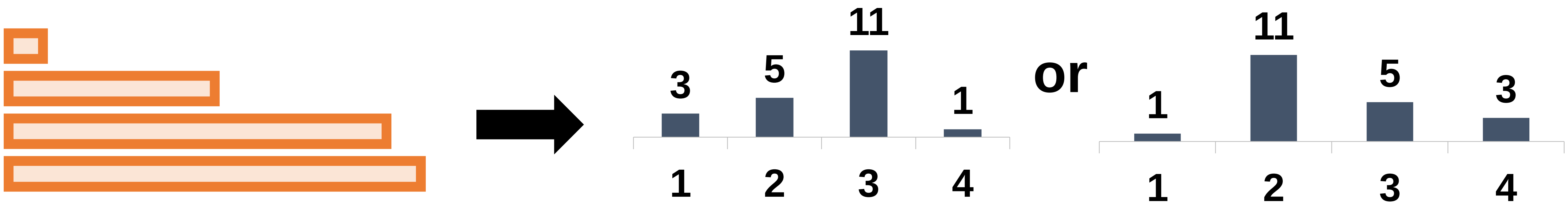
Done!

set of all observed volumes: 1, 3, 5, 8, 11, 12, 16, 17, 19, 20

Exploiting Volume Leakage



- **Build** a graph using all observed volumes
- Use properties of range queries to identify **elementary** volumes, which form a clique
- Use elementary volumes to directly **reconstruct** all counts in the database



How Many Queries Are Needed?

Suppose values in $\{1, \ldots, N\}$, queries drawn equally at random.

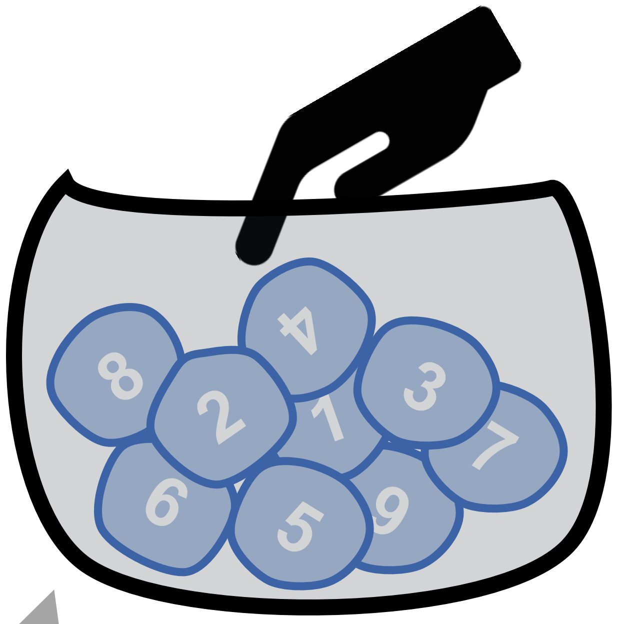
How Many Queries Are Needed?

Suppose values in {1, …, N}, queries drawn equally at random.

N^2 log N queries expected to see **all volumes**

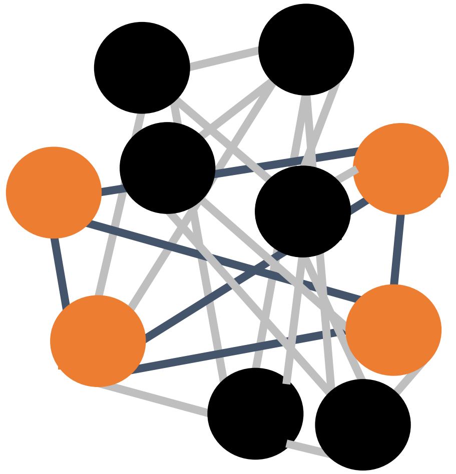
Coupon collector bound

- **Q:** How many random draws expected till all coupons have been drawn at least once?
- **A:** ≈ $N^2 \log N$



N(N+1)/2 "coupons"
(one for every range)

Exploiting Volume Leakage



- **Build** a graph using all observed volumes
- Use properties of range queries to identify **elementary** volumes, which form a clique
- Use elementary volumes to directly **reconstruct** all counts in the database

Details: [Grubbs, Lacharité, Minaud, and Paterson, CCS 2018]

Outline

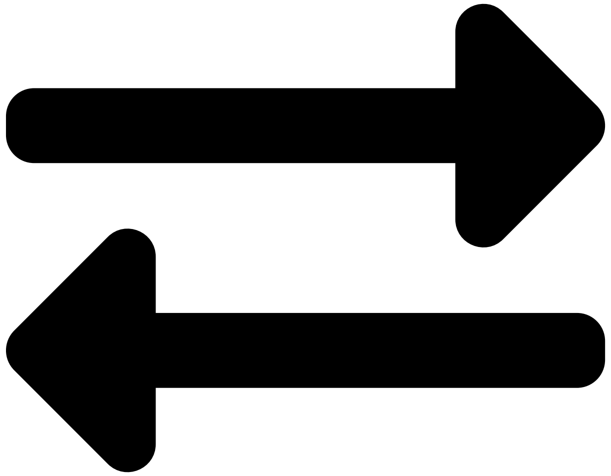
1. Existing approaches to securing a database
   - Securing data in transit, at rest, and in use

2. How to exploit leakage to break database encryption
   - Exploiting access pattern leakage and volume leakage

3. Security recommendations
   - Types of leakage, leaky operations, trade-offs

Approach

What can leak?



Where and **when** can it leak?

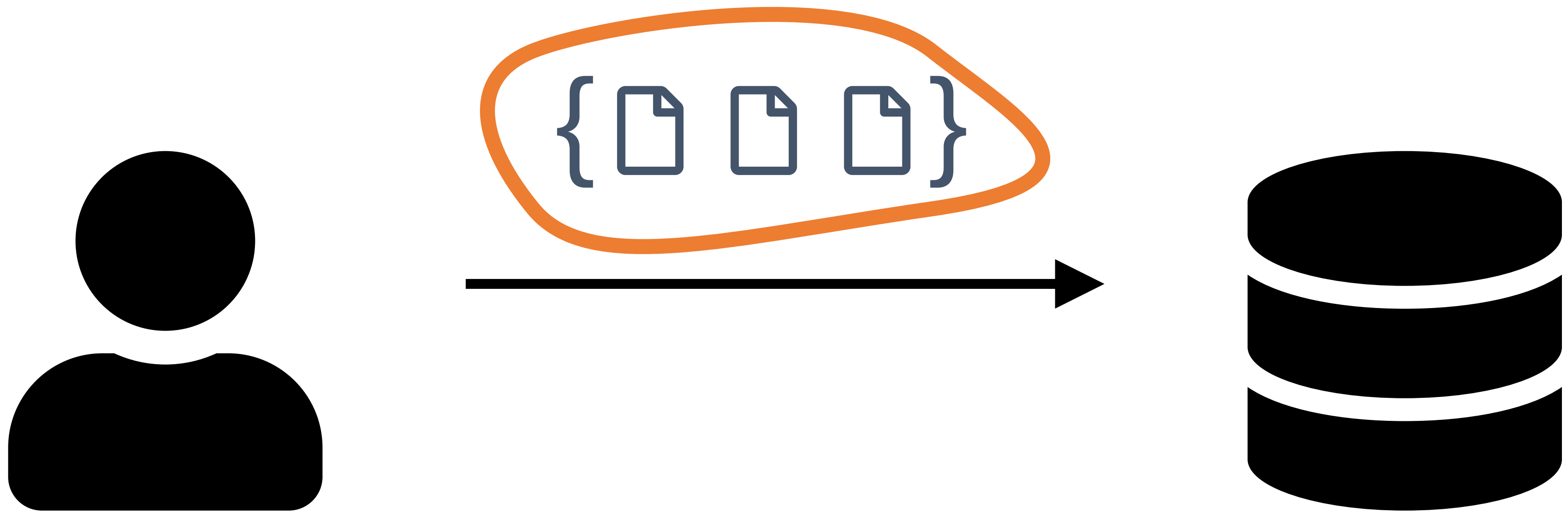
What Can Leak?

Properties related to…

- **Values:** order, distance, existence, number of distinct values, repetition, …
- **Queries:** endpoints, repetition, width, inclusion, …
- **Responses:** which rows matched, how many rows matched, repetition, …

[Kamara et al., CRYPTO 2018]

Where and When Can It Leak?

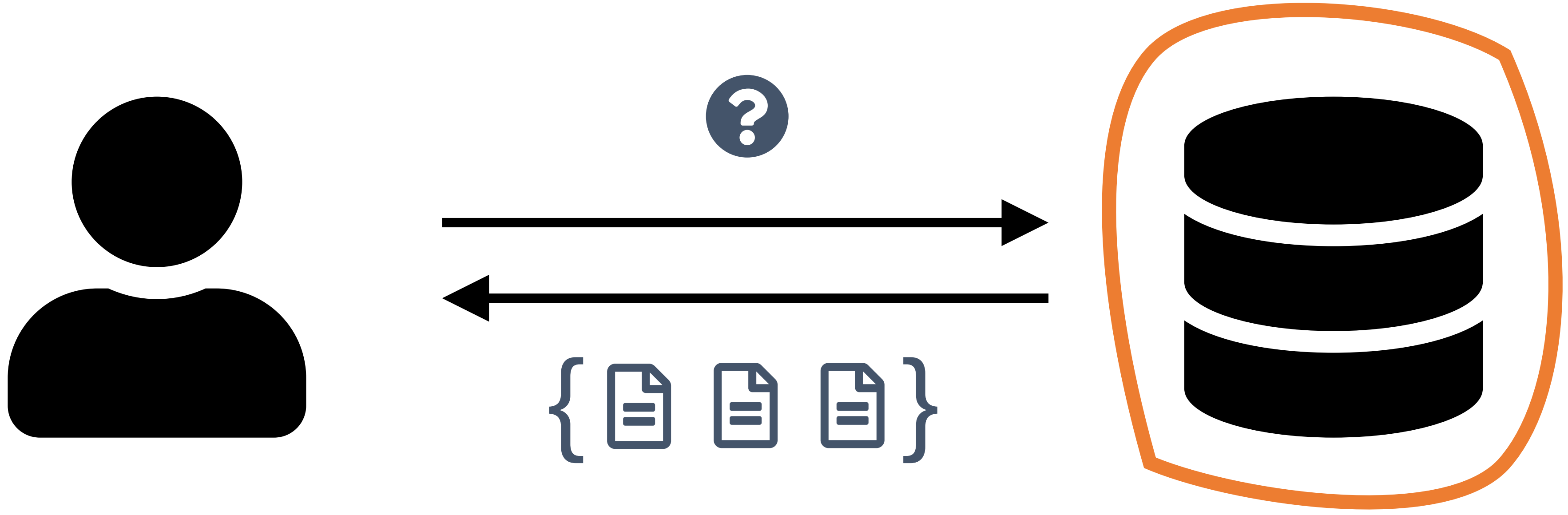


	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Where and When Can It Leak?

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Where and When Can It Leak?



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Trade-offs

Trade-offs

MITIGATION TECHNIQUES

- Restricting query types
- Dummy records
- Dummy values
- Trusting hardware
- …

Trade-offs

MITIGATION TECHNIQUES

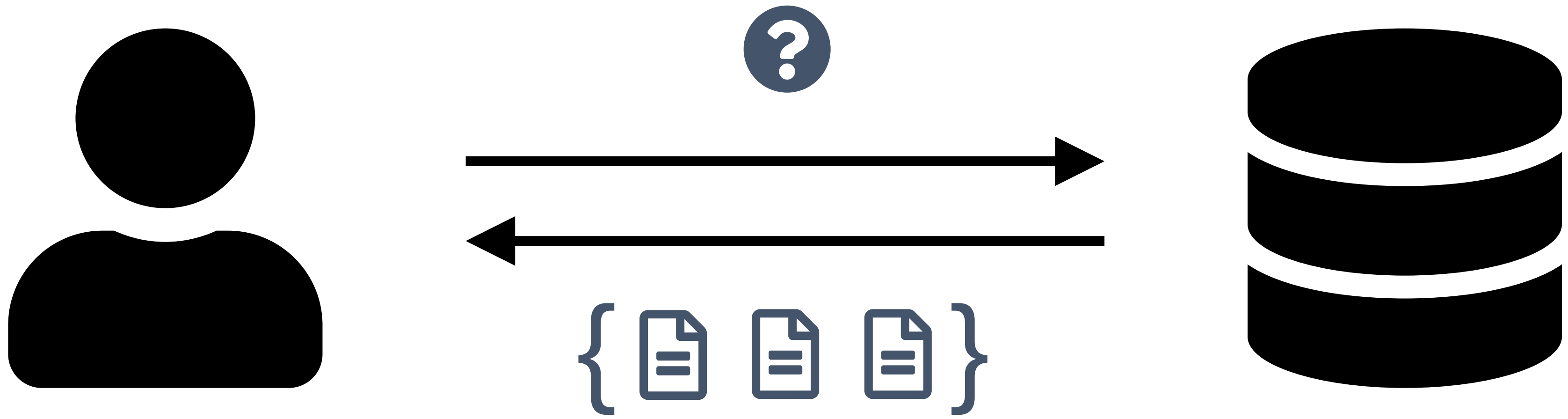
- Restricting query types
- Dummy records
- Dummy values
- Trusting hardware
- …

COSTS

- Incomplete results
- Probabilistically correct results
- Efficiency
- Less compression/deduplication
- …

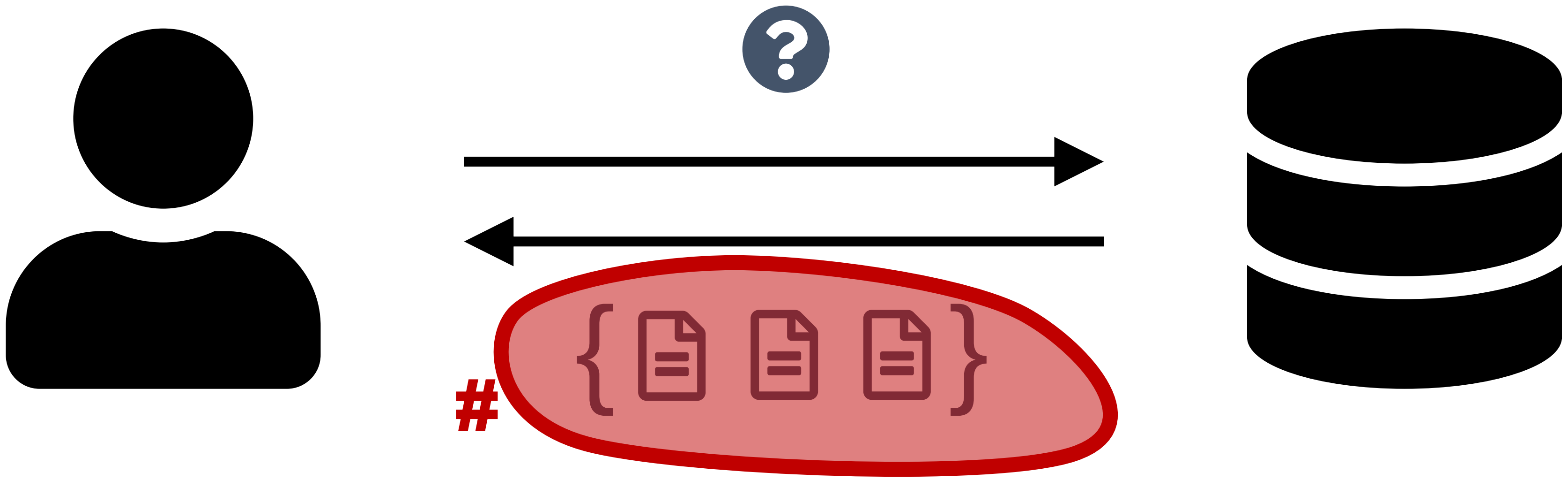
Conclusion

Encrypted Databases



	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypted Databases

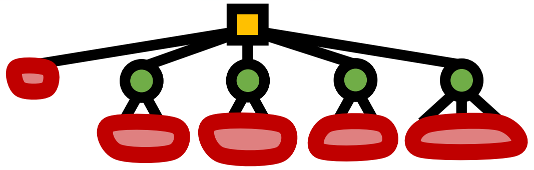


volume leakage
(*how many* records)

access pattern leakage
(*which* records)

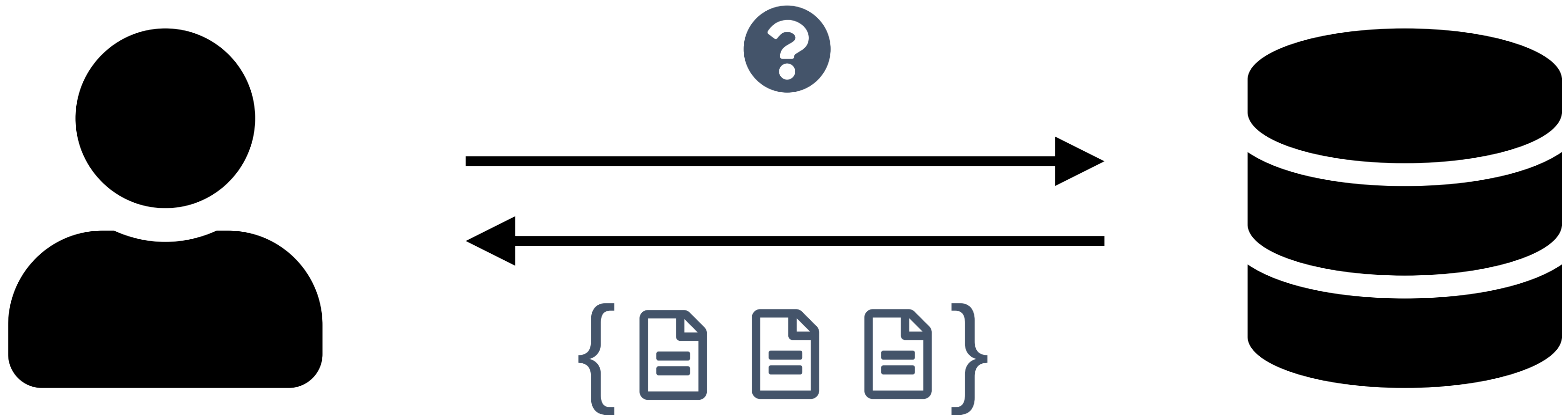
	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypted Databases

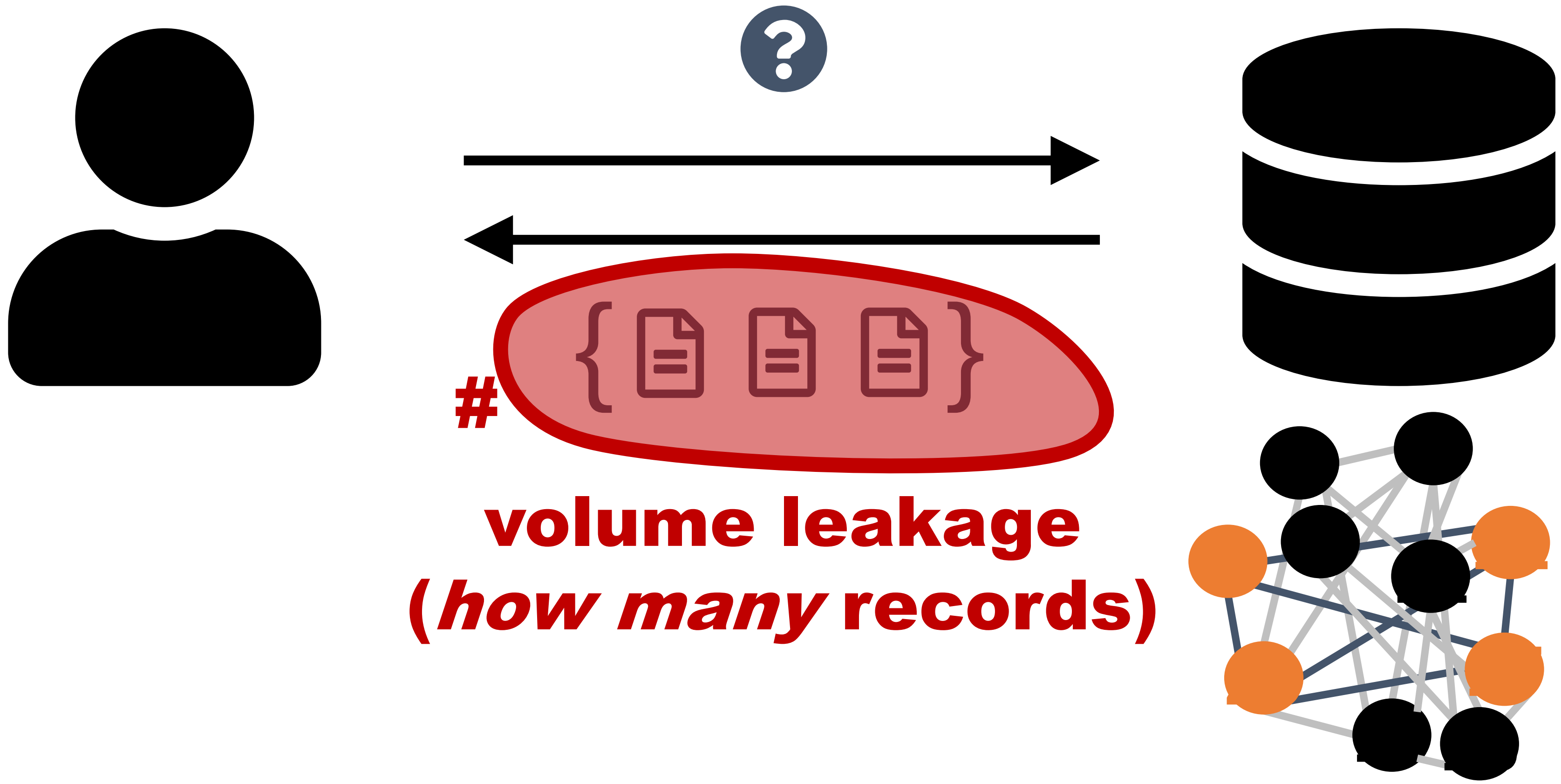


access pattern leakage
(*which* records)

	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
...	...	...

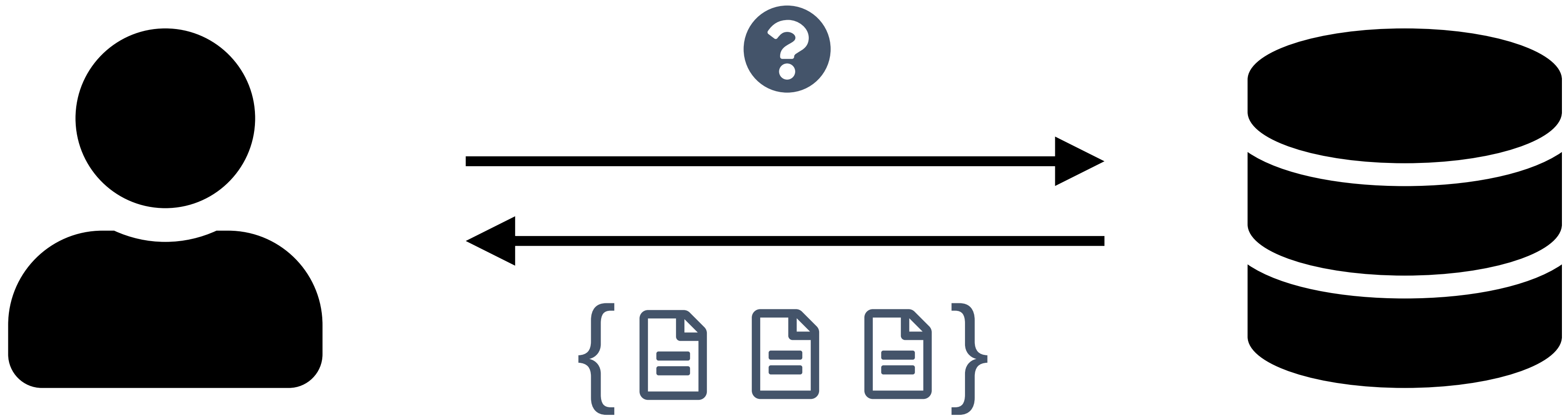


Encrypted Databases



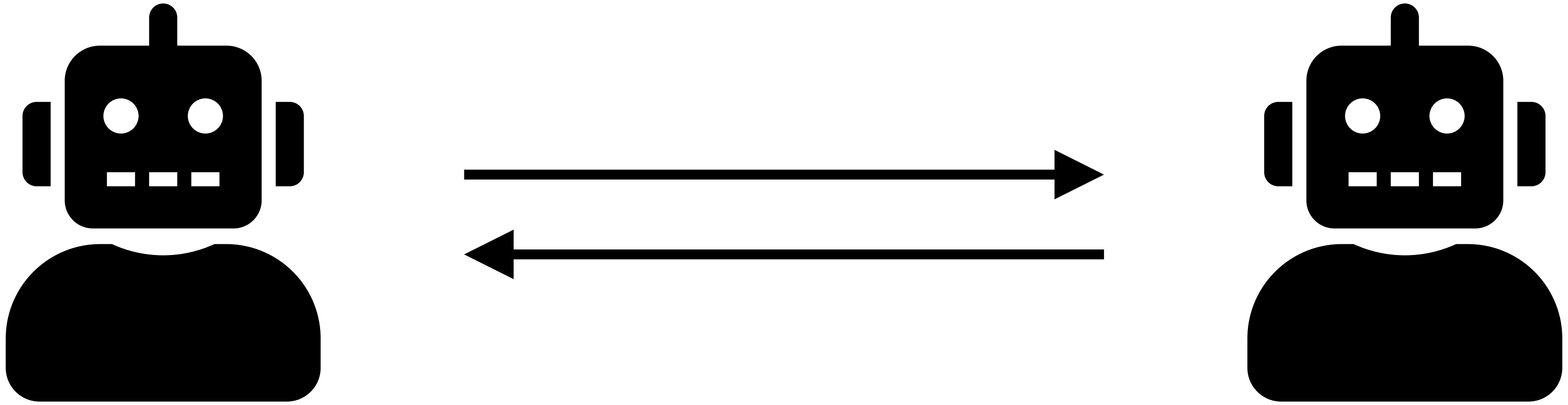
	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

Encrypted Databases

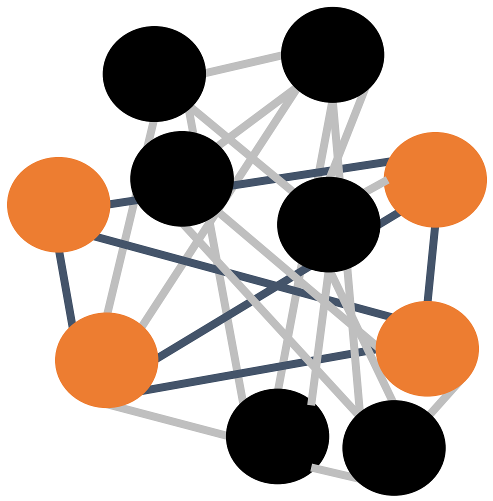


	ID	Value
	1	3
	2	1
	3	15
	4	41
	5	1
…	…	…

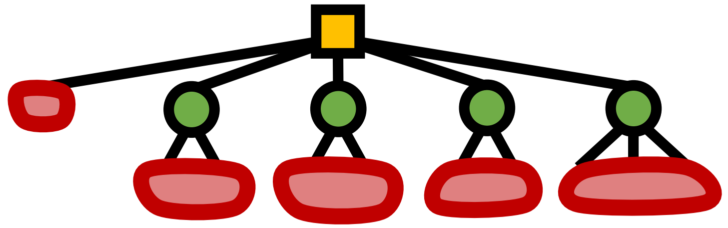
Side Channel Attacks



Thank you!



Questions?



mariesarah.lacharite@gmail.com
@znevrfnenu

Black Hat Sound Bytes

- Databases have many unique side channels that leak information.
- Side channel attacks exploiting this leakage can break encryption.
- Understanding different kinds of leakage and during what operations they arise can help secure an encrypted database.