Predicate Encryption for Multi-Dimensional Range Queries from Lattices

Romain GAY, Pierrick MÉAUX, Hoeteck WEE

École Normale Supérieure, CNRS, INRIA, PSL, Paris, France

PKC 2015 — Maryland, USA
Wednesday, April 1

Online Dating

Profile

Alice

Header

Hobbies

Pictures

Online Dating

Profile

Alice
Header
Hobbies
Pictures

Alice's preferences

N pictures:

$$x_1 > 0$$

Children:

$$x_2 = 0$$

Age:

$$24 \leq x_3 \leq 36$$

Salary:

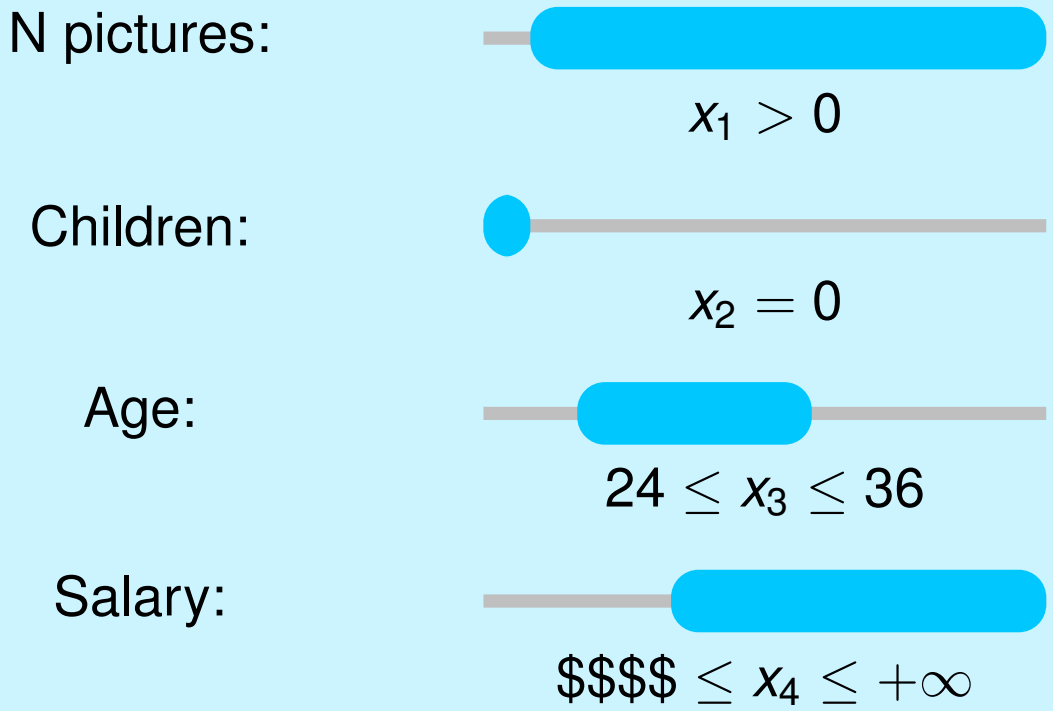
$$\$\$\$ \leq x_4 \leq +\infty$$

Online Dating

Profile

Alice
Header
Hobbies
Pictures

Alice's preferences



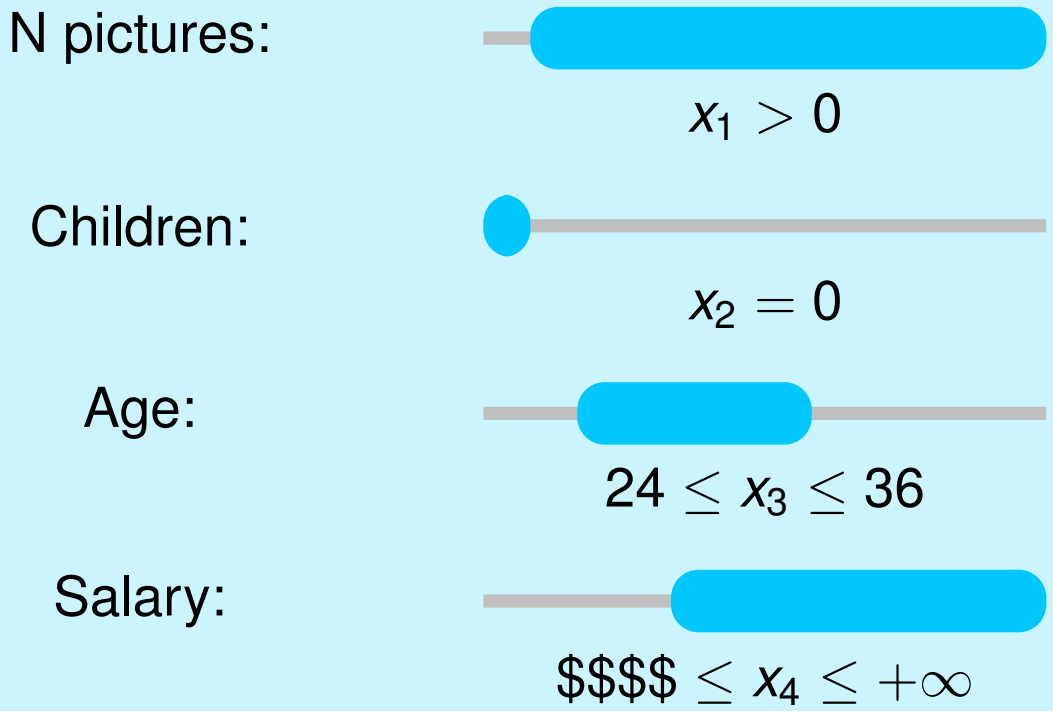
Online dating as Multi Dimensional Range Queries (MDRQ)

Online Dating

Profile

Alice
Header
Hobbies
Pictures

Alice's preferences



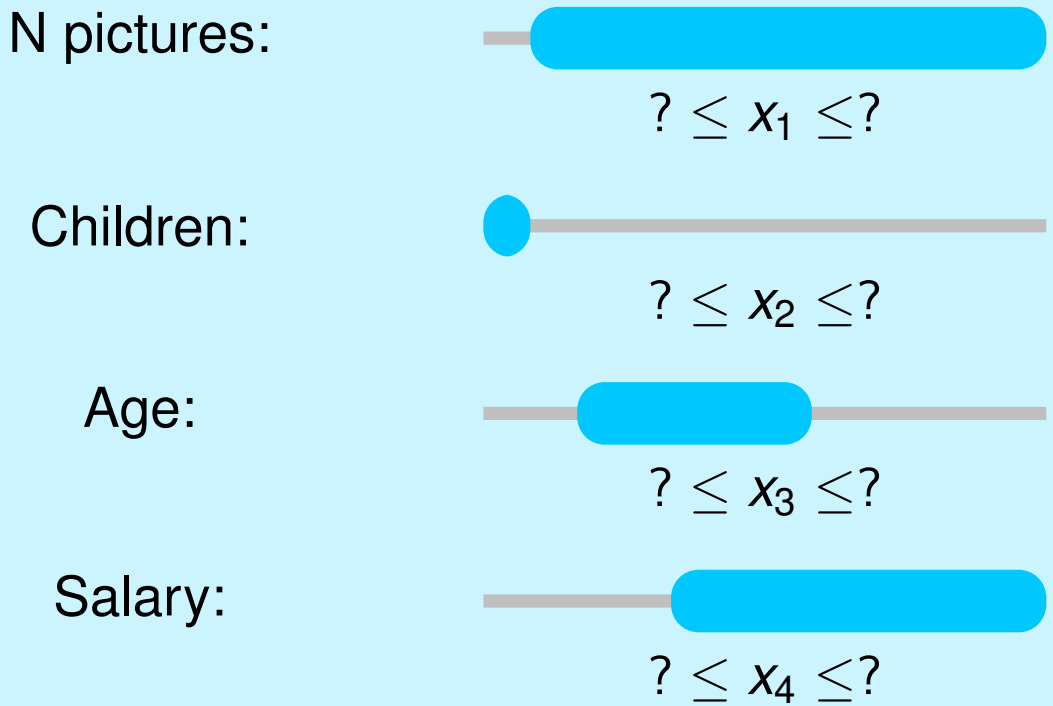
Online dating using Attribute-Based Encryption [SW05, GPSW06, GVW13]

Online Dating

Profile

Alice
Header
Hobbies
Pictures

Alice's preferences



ABE hides profile but not preferences

Online Dating

Profile

Alice
Header
Hobbies
Pictures

Alice's preferences

N pictures: $? \leq x_1 \leq ?$

Children: $? \leq x_2 \leq ?$

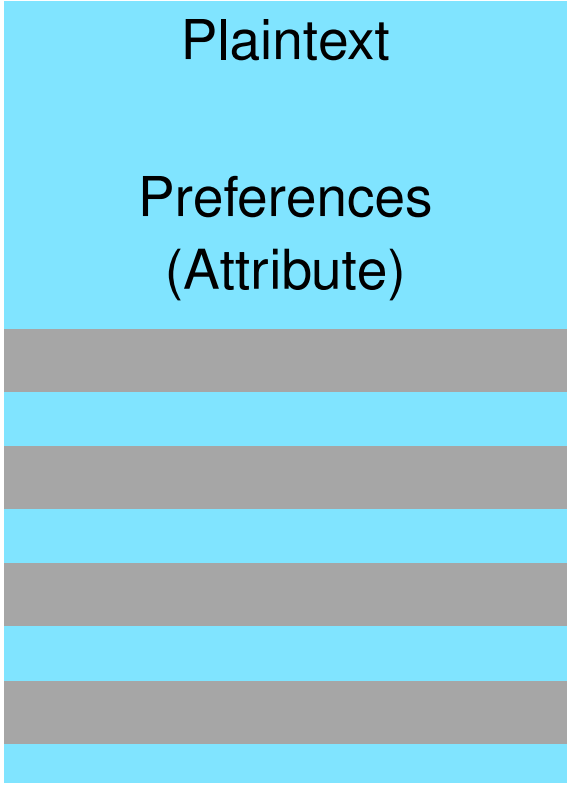
Age: $? \leq x_3 \leq ?$

Salary: $? \leq x_4 \leq ?$

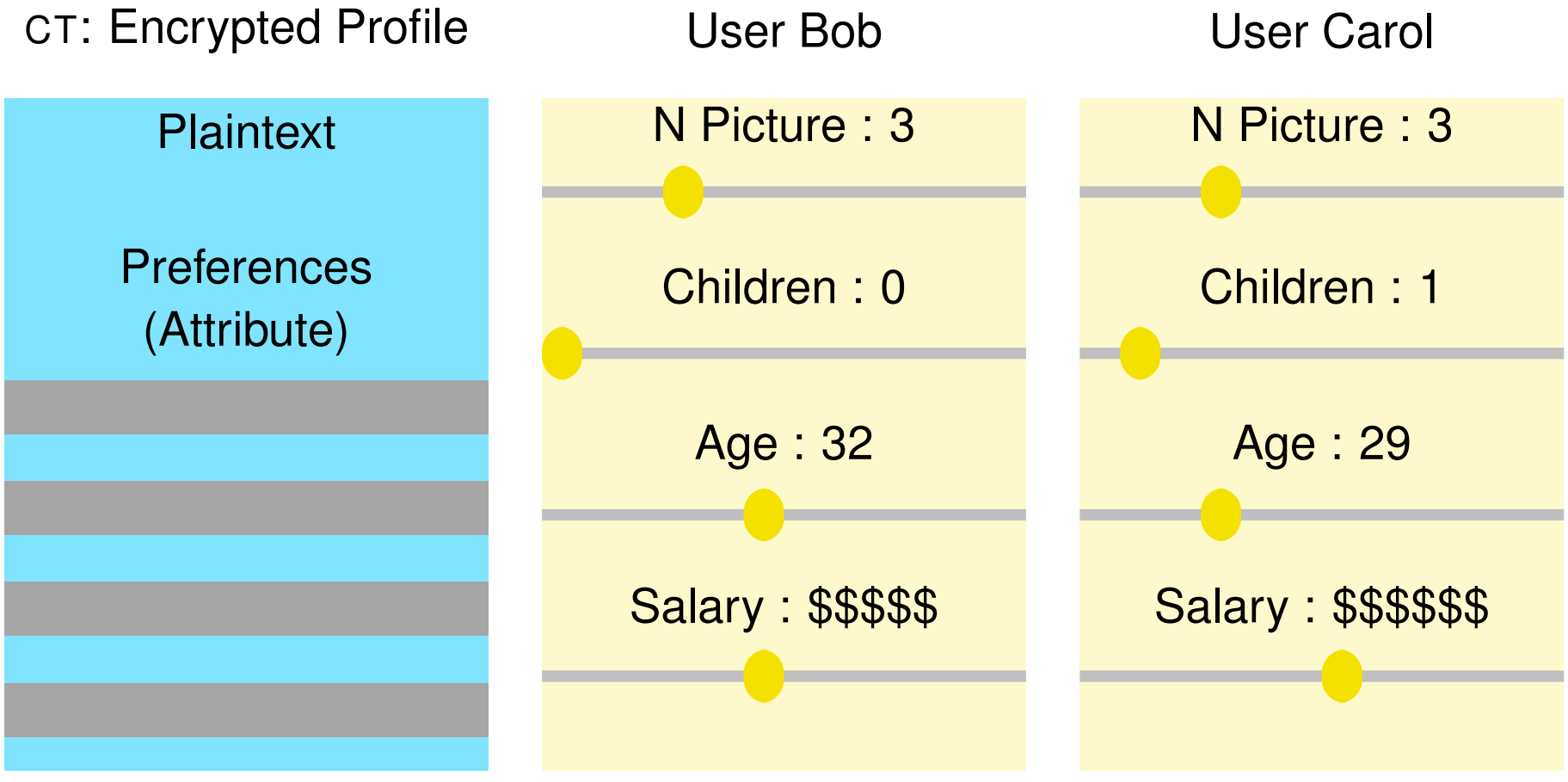
Online dating using Predicate Encryption [BW07, SBC+07,KSW08]

Online Dating Encryption Scheme

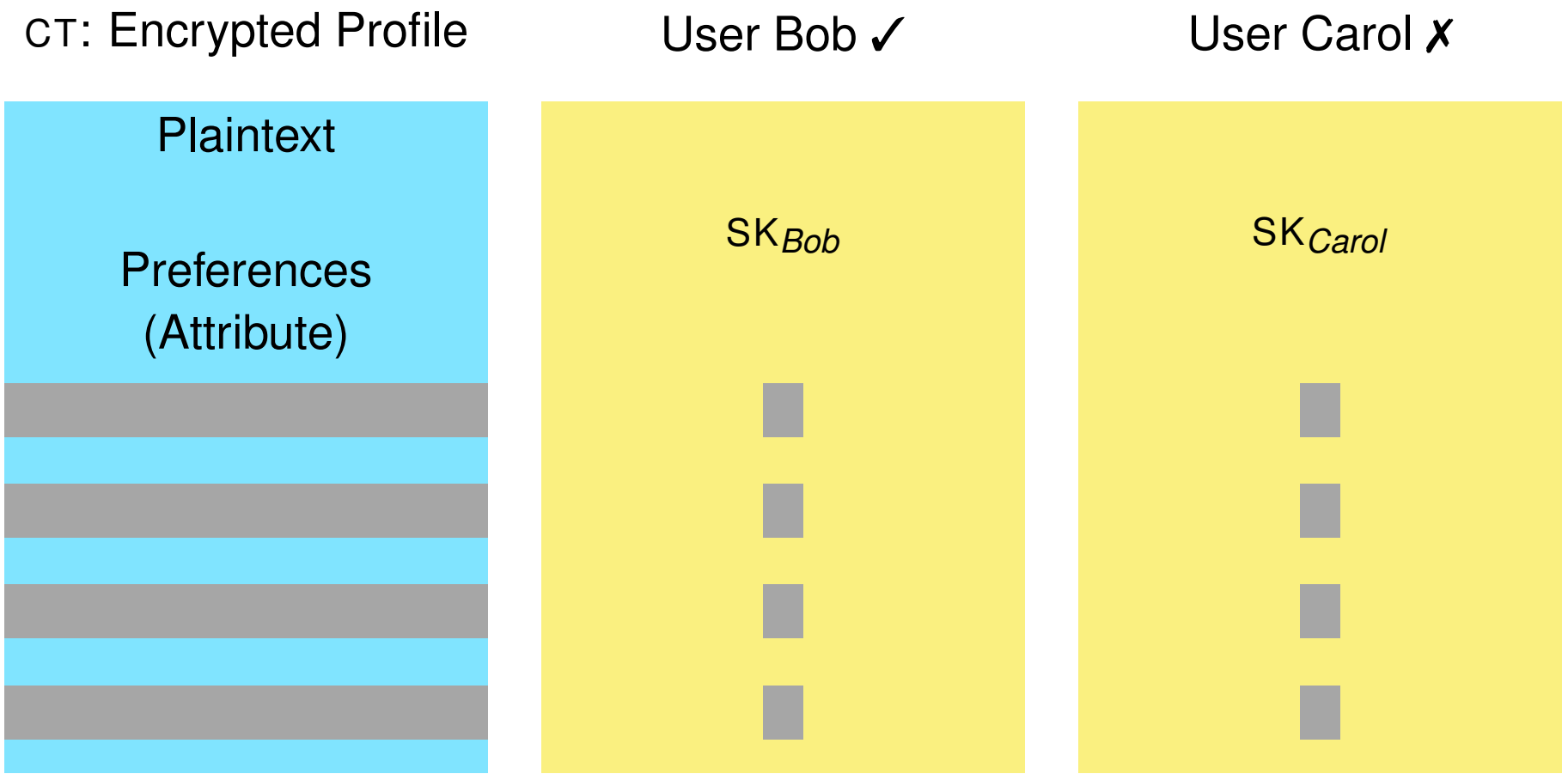
CT: Encrypted Profile



Online Dating Encryption Scheme

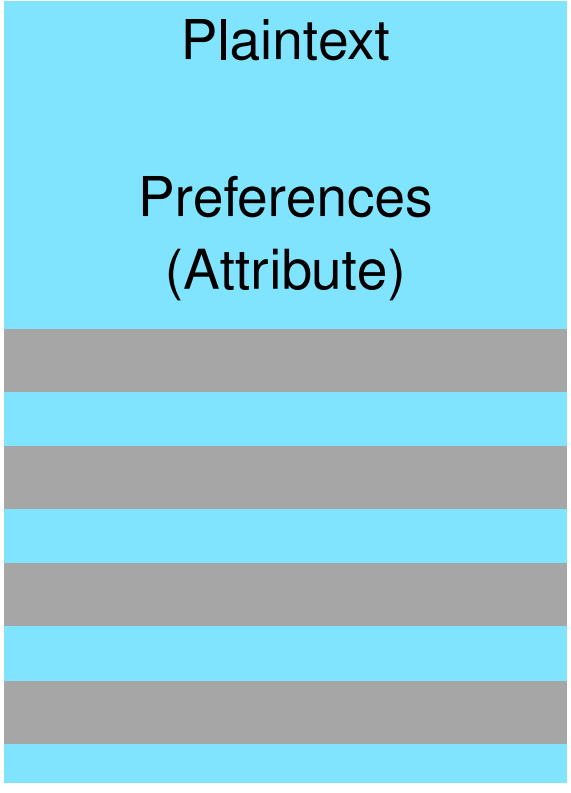


Online Dating Encryption Scheme

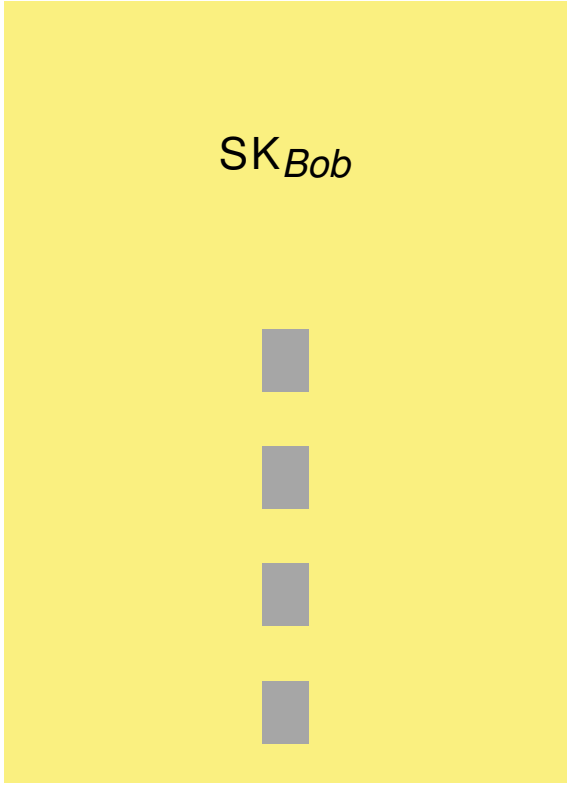


Online Dating Encryption Scheme

CT: Encrypted Profile



User Bob ✓



Decryption

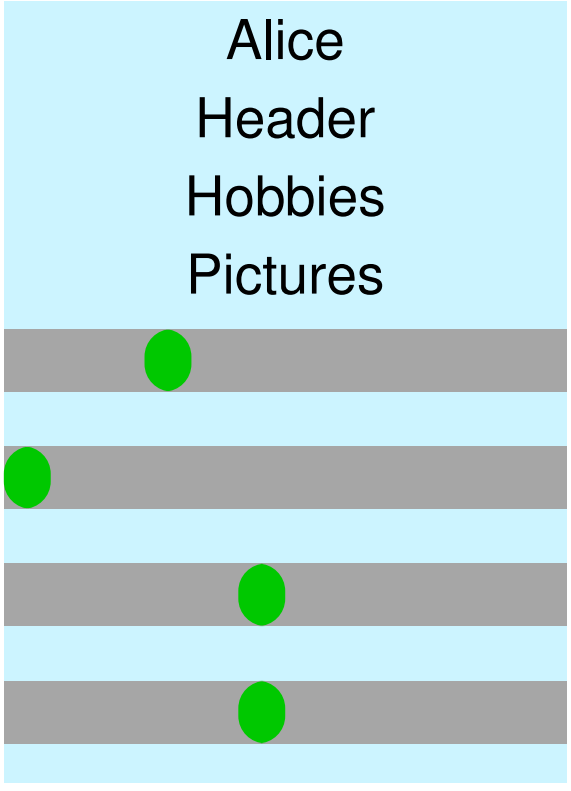
User matching

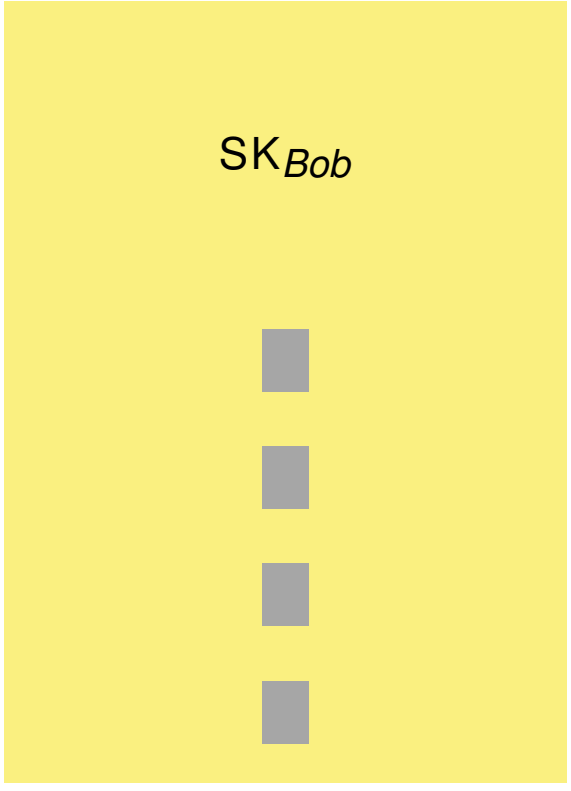
the preferences ✓

Online Dating Encryption Scheme

m : Decrypted Profile

User Bob ✓





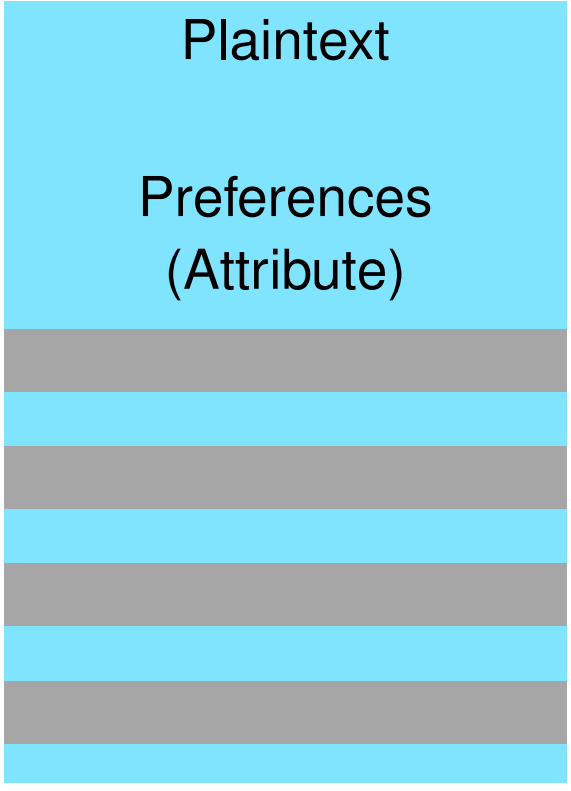
User matching

the preferences ✓

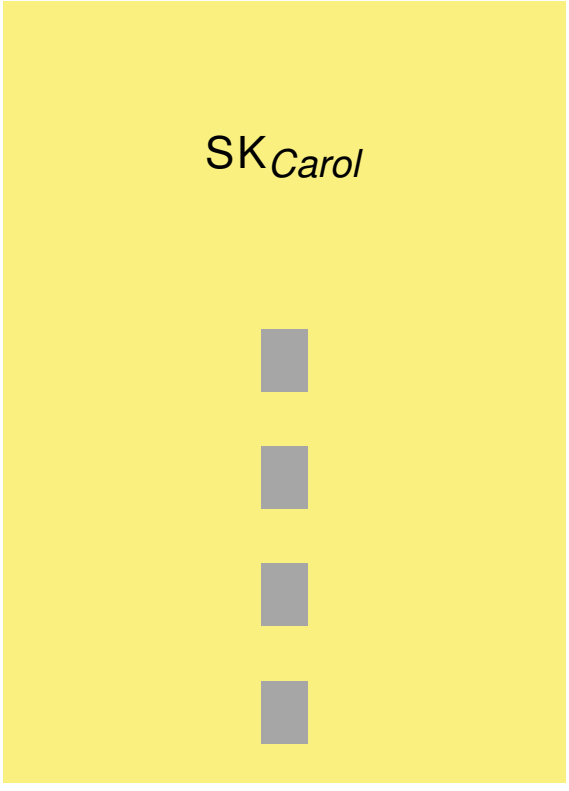
Successful decryption and learning the matches

Online Dating Encryption Scheme

CT: Encrypted Profile



User Carol ✗



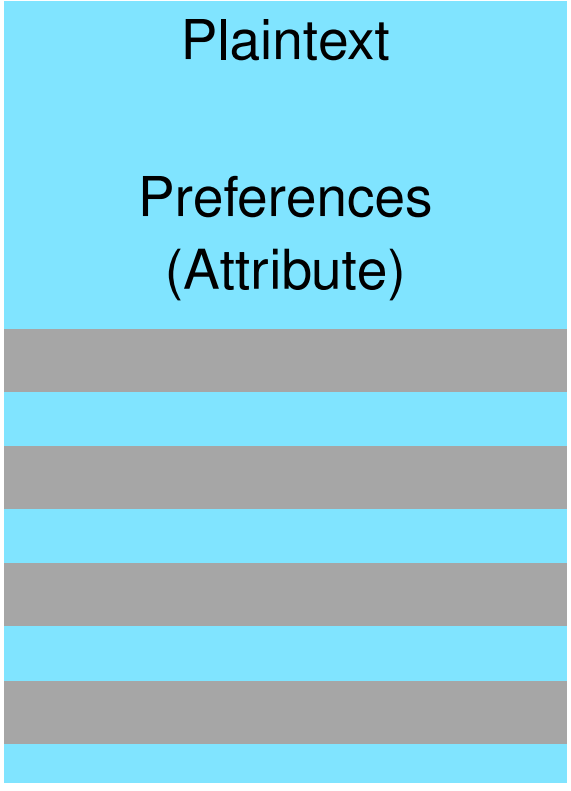
User not matching

the preferences ✗

Decryption

Online Dating Encryption Scheme

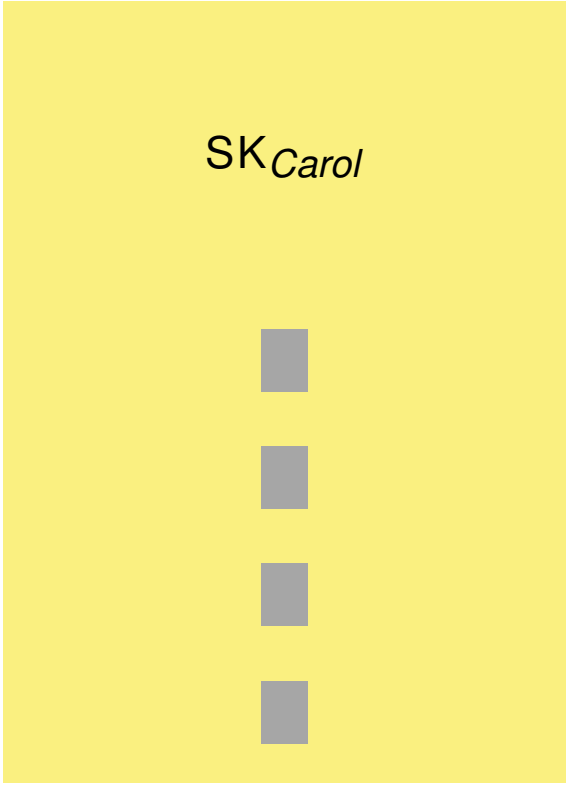
CT: Encrypted Profile



User not matching

the preferences ✗

User Carol ✗



Unauthorised decryption, no more information

A Predicate for Online Dating

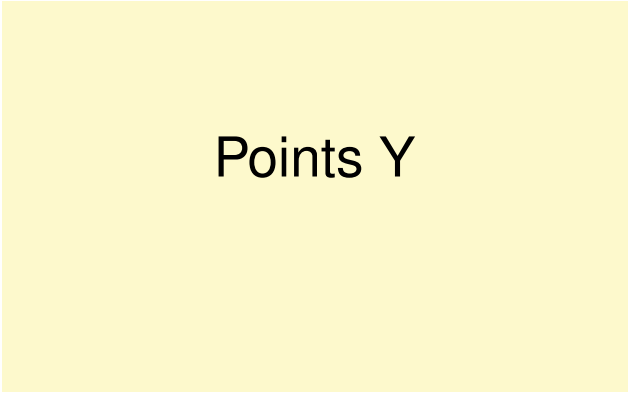
Matching preferences $\rightarrow$ MDRQ

A Predicate for Online Dating

Matching preferences $\rightarrow$ MDRQ

Preferences

User



A Predicate for Online Dating

Matching preferences $\rightarrow$ MDRQ

Preferences

User

Predicate on X and Y

A Predicate for Online Dating

Matching preferences $\rightarrow$ MDRQ

Preferences

User

Predicate on X and Y

Points into Ranges

$P(X, Y) = 1$

$\Downarrow$

Authorised decryption

A Predicate for Online Dating

Matching preferences $\rightarrow$ MDRQ

Preferences

User

Predicate on X and Y

Points not into Ranges

$P(X, Y) = 0$

$\Downarrow$

Unauthorised decryption

Result

Theorem

Predicate Encryption
for
MDRQ
from
LWE

Prior works

from pairings
[BW07,SBC+07]

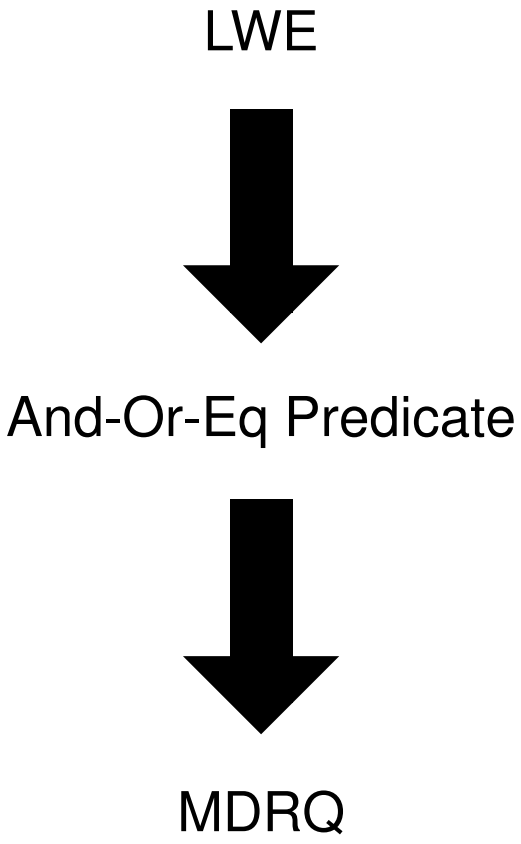
Result

Theorem

Predicate Encryption
for
MDRQ
from
LWE

Prior works

from pairings
[BW07,SBC+07]



Or Eq Predicate

Conjunction of equality queries

$\mathsf{P}_{\text{OR-EQ}} : \mathbb{Z}_q^\ell \times \mathbb{Z}_q^\ell \to \{0,1\}$

$\mathsf{P}_{\text{OR-EQ}}(\mathbf{x},\mathbf{y}) = \bigvee_{j=1}^{\ell} (\mathbf{x}_j = \mathbf{y}_j)$

Vector **x**

1	2	3	4	5

Vector **y**

5	4	3	2	1

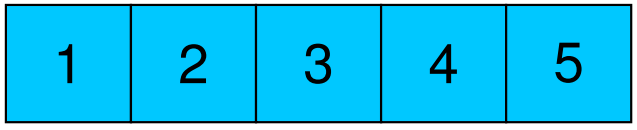
Or Eq Predicate

Conjunction of equality queries

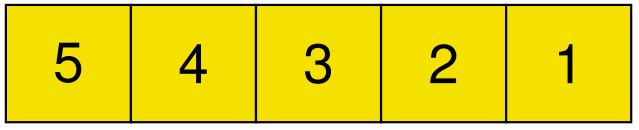
$\mathsf{P}_{\text{OR-EQ}} : \mathbb{Z}_q^\ell \times \mathbb{Z}_q^\ell \to \{0,1\}$

$\mathsf{P}_{\text{OR-EQ}}(\mathbf{x},\mathbf{y}) = \bigvee_{j=1}^{\ell} (\mathbf{x}_j = \mathbf{y}_j)$

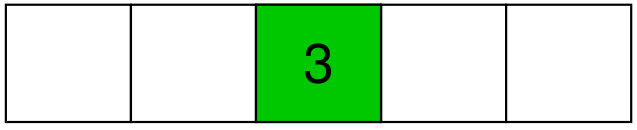
Vector **x**



Vector **y**



Equality match

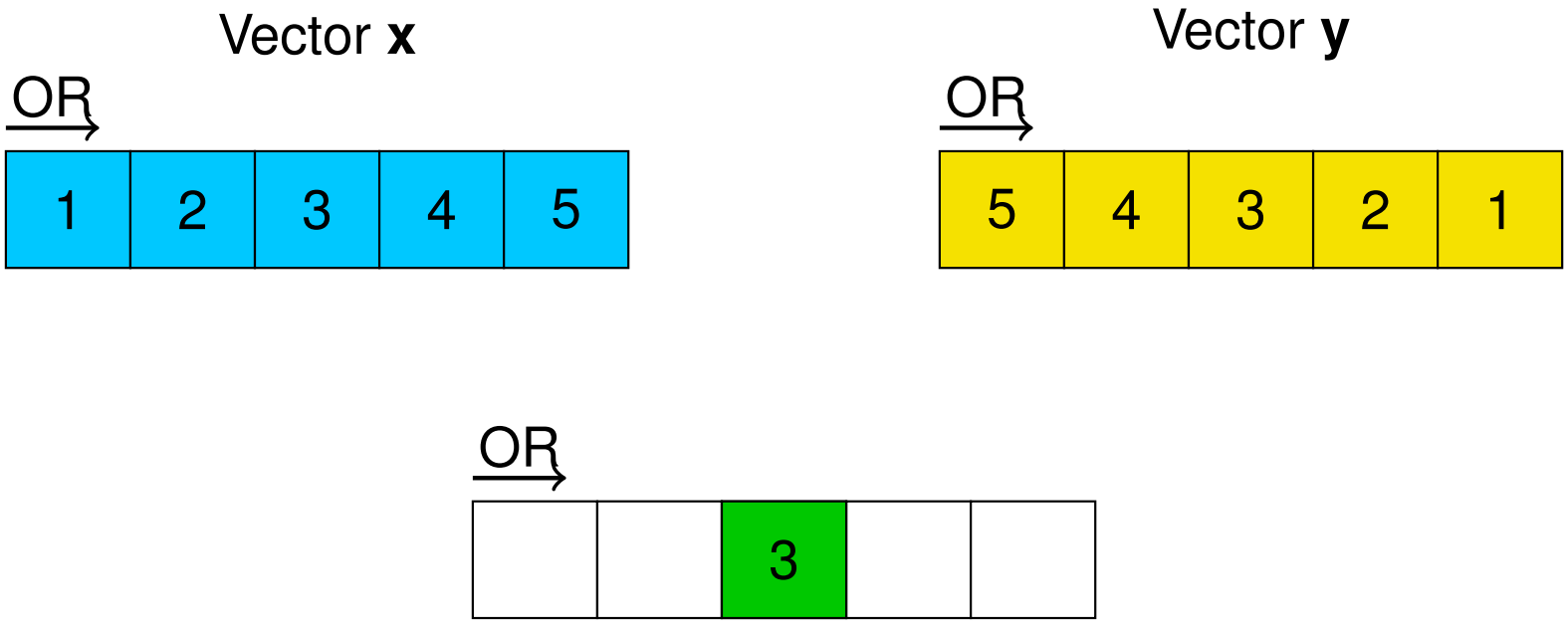


Or Eq Predicate

Conjunction of equality queries

$\mathsf{P}_{\text{OR-EQ}} : \mathbb{Z}_q^\ell \times \mathbb{Z}_q^\ell \to \{0,1\}$

$\mathsf{P}_{\text{OR-EQ}}(\mathbf{x},\mathbf{y}) = \bigvee_{j=1}^{\ell}(\mathbf{x}_j = \mathbf{y}_j)$



$\mathsf{P}_{\text{OR-EQ}}(\mathbf{x},\mathbf{y}) = 1$

Or Eq Predicate

Conjunction of equality queries

$\mathsf{P}_{\text{OR-EQ}} : \mathbb{Z}_q^\ell \times \mathbb{Z}_q^\ell \to \{0,1\}$

$\mathsf{P}_{\text{OR-EQ}}(\mathbf{x},\mathbf{y}) = \bigvee_{j=1}^{\ell}(\mathbf{x}_j = \mathbf{y}_j)$

Vector $\mathbf{x}$

1	2	3	4	5

Vector $\mathbf{y}'$

2	3	4	5	1

Or Eq Predicate

Conjunction of equality queries

$\mathsf{P}_{\text{OR-EQ}} : \mathbb{Z}_q^\ell \times \mathbb{Z}_q^\ell \to \{0,1\}$

$\mathsf{P}_{\text{OR-EQ}}(\mathbf{x},\mathbf{y}) = \bigvee_{j=1}^{\ell} (\mathbf{x}_j = \mathbf{y}_j)$

Vector $\mathbf{x}$

1	2	3	4	5

Vector $\mathbf{y}'$

2	3	4	5	1

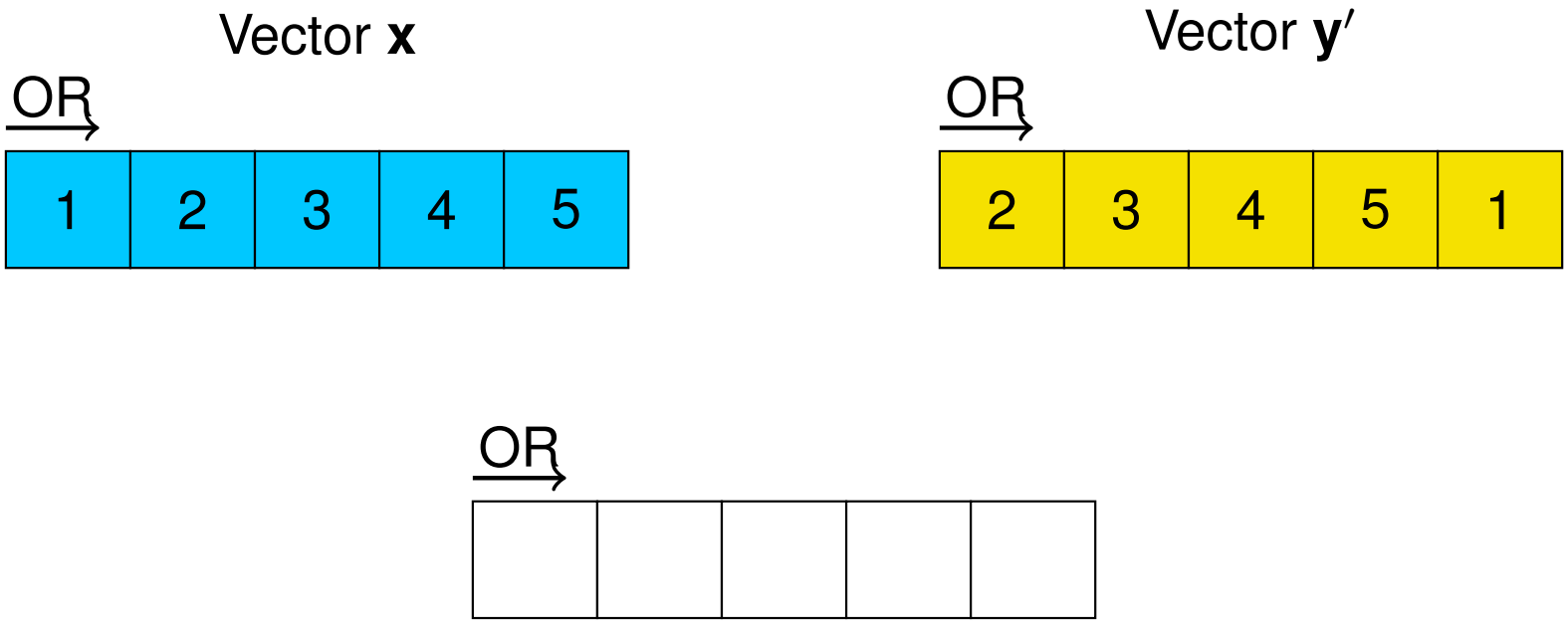
Equality match

Or Eq Predicate

Conjunction of equality queries

$\mathsf{P}_{\text{OR-EQ}} : \mathbb{Z}_q^\ell \times \mathbb{Z}_q^\ell \to \{0,1\}$

$\mathsf{P}_{\text{OR-EQ}}(\mathbf{x},\mathbf{y}) = \bigvee_{j=1}^{\ell} (\mathbf{x}_j = \mathbf{y}_j)$



$\mathsf{P}_{\text{OR-EQ}}(\mathbf{x},\mathbf{y}') = 0$

And Or Eq Predicate

Disjunction of Conjunction of equality queries

$\mathsf{P}_{\text{AND-OR-EQ}} : \mathbb{Z}_q^{D \times \ell} \times \mathbb{Z}_q^{D \times \ell} \to \{0, 1\}$

$\mathsf{P}_{\text{AND-OR-EQ}}(X, Y) = \bigwedge_{i=1}^{D} \bigvee_{j=1}^{\ell} (X_{i,j} = Y_{i,j})$

Matrix X

1	2	3	4	5
2	3	4	5	1

Matrix Y

5	4	3	2	1
4	3	2	1	5

And Or Eq Predicate

Disjunction of Conjunction of equality queries

$\mathsf{P}_{\text{AND-OR-EQ}} : \mathbb{Z}_q^{D\times\ell} \times \mathbb{Z}_q^{D\times\ell} \to \{0,1\}$

$\mathsf{P}_{\text{AND-OR-EQ}}(X, Y) = \bigwedge_{i=1}^{D} \bigvee_{j=1}^{\ell} (X_{i,j} = Y_{i,j})$

Matrix X

1	2	3	4	5
2	3	4	5	1

Matrix Y

5	4	3	2	1
4	3	2	1	5

Equality match

		3		
	3			

And Or Eq Predicate

Disjunction of Conjunction of equality queries

$$P_{\text{AND-OR-EQ}} : \mathbb{Z}_q^{D \times \ell} \times \mathbb{Z}_q^{D \times \ell} \to \{0, 1\}$$

$$P_{\text{AND-OR-EQ}}(X, Y) = \bigwedge_{i=1}^{D} \bigvee_{j=1}^{\ell} (X_{i,j} = Y_{i,j})$$

Matrix X

OR →

1	2	3	4	5
2	3	4	5	1

Matrix Y

OR →

5	4	3	2	1
4	3	2	1	5

OR →

		3		
	3			

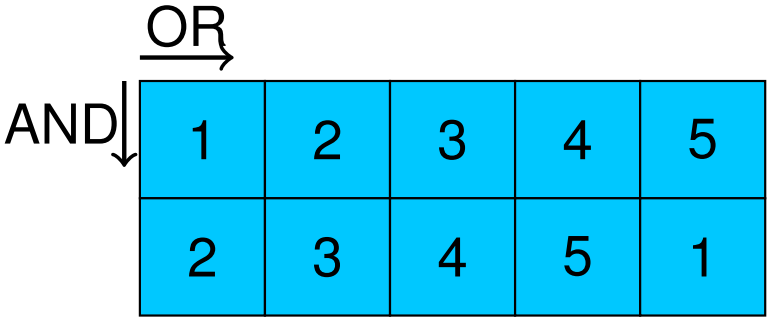
And Or Eq Predicate

Disjunction of Conjunction of equality queries

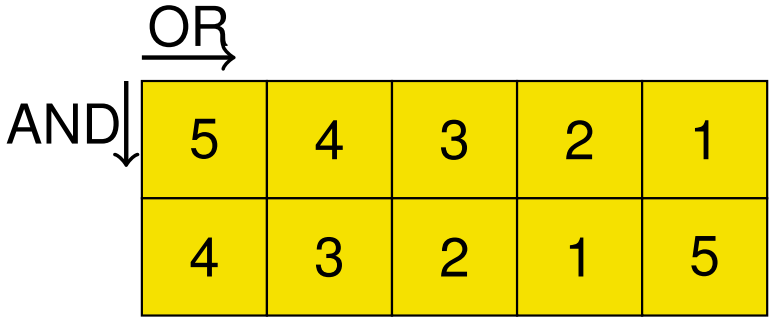
$\mathsf{P}_{\text{AND-OR-EQ}} : \mathbb{Z}_q^{D\times\ell} \times \mathbb{Z}_q^{D\times\ell} \to \{0,1\}$

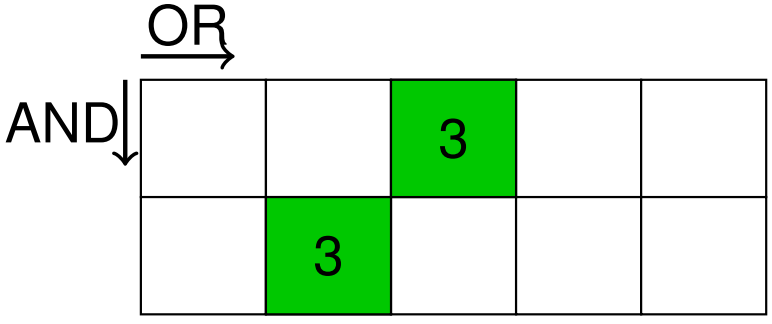
$\mathsf{P}_{\text{AND-OR-EQ}}(X, Y) = \bigwedge_{i=1}^{D} \bigvee_{j=1}^{\ell} (X_{i,j} = Y_{i,j})$

Matrix X



Matrix Y



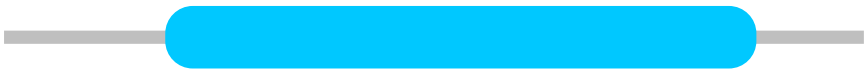


$\mathsf{P}_{\text{AND-OR-EQ}}(X, Y) = 1$

From One-dimensional Range Query to Or Eq

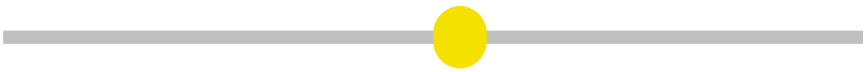
Range X

$X = [3, 13]$



Point Y

$Y = 8$

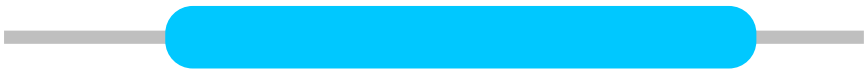


$P_{\text{OR EQ}}(\mathbf{x}, \mathbf{y}) = ?$

From One-dimensional Range Query to Or Eq

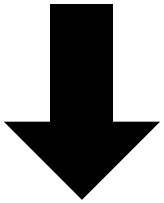
Range X

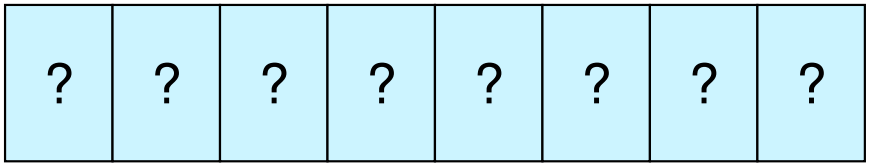
$X = [3, 13]$



Point Y

$Y = 8$



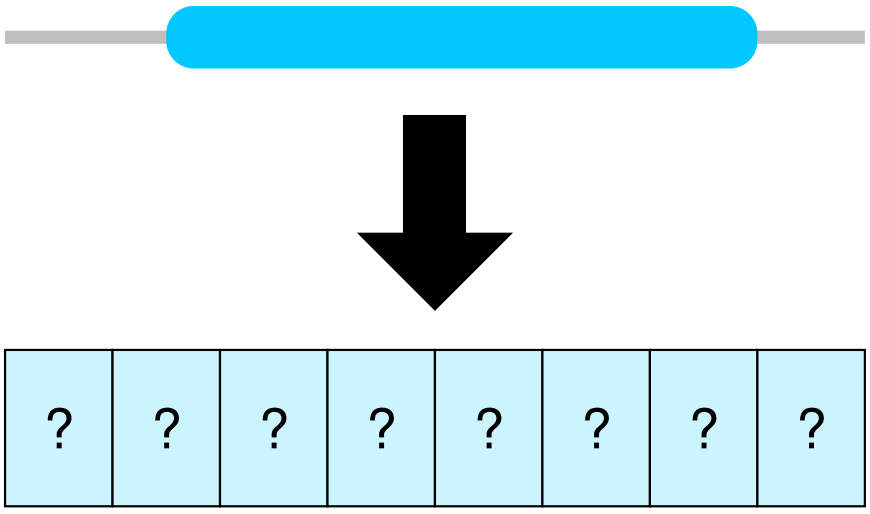


$P_{\text{OR EQ}}(\mathbf{x}, \mathbf{y}) = ?$

From One-dimensional Range Query to Or Eq

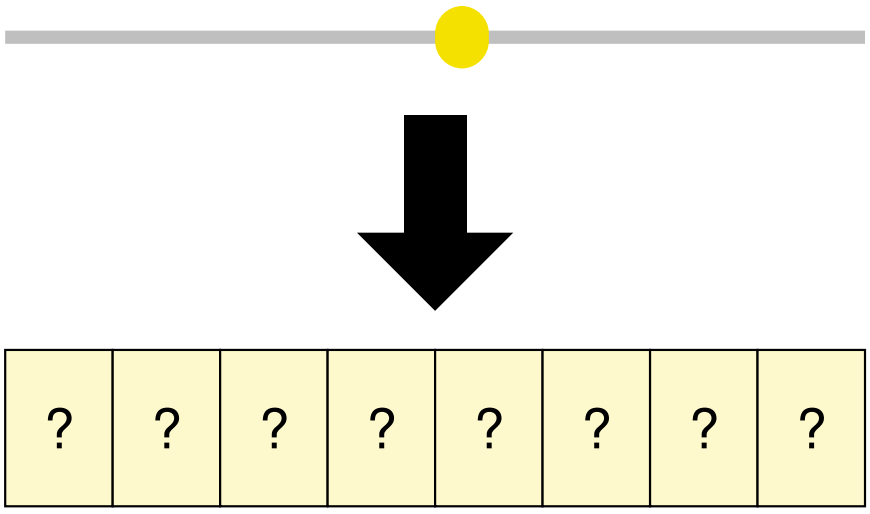
Range X

$X = [3, 13]$



Point Y

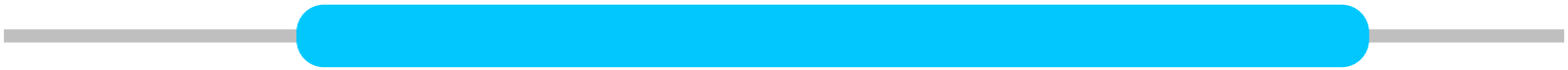
$Y = 8$



$P_{\text{OR EQ}}(\mathbf{x}, \mathbf{y}) = ?$

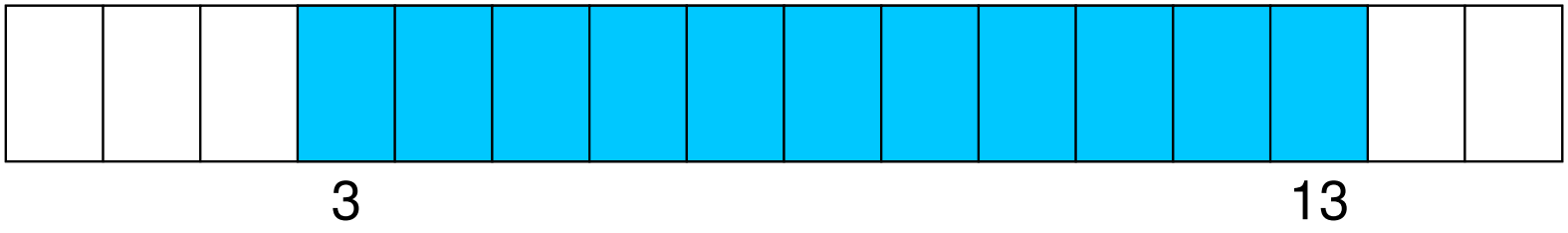
From Range to Vector

Query over $[0, 2^{\ell} - 1]$



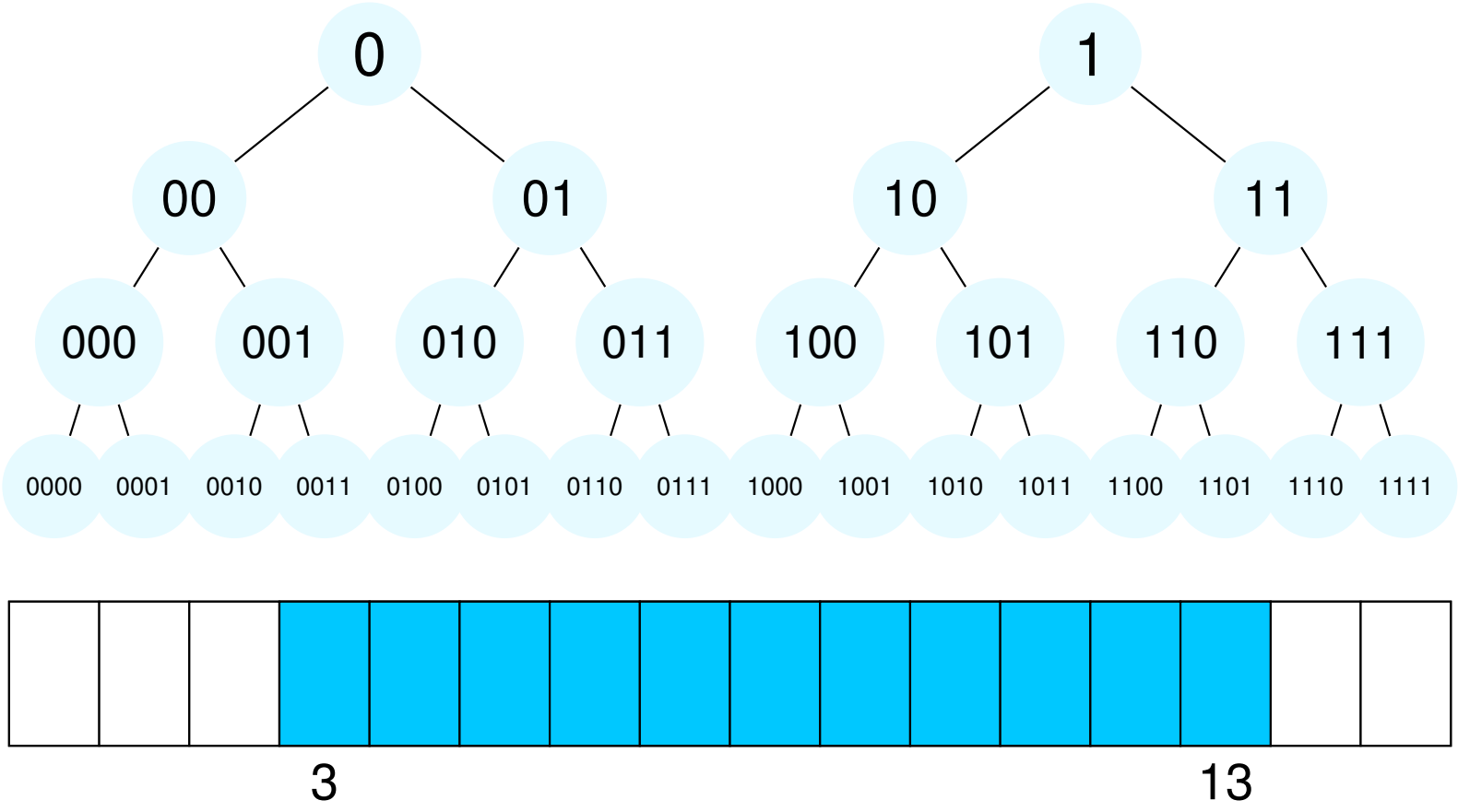
From Range to Vector

Query over $[0, 2^\ell - 1]$; example: $\ell = 4$, range $= [3, 13]$



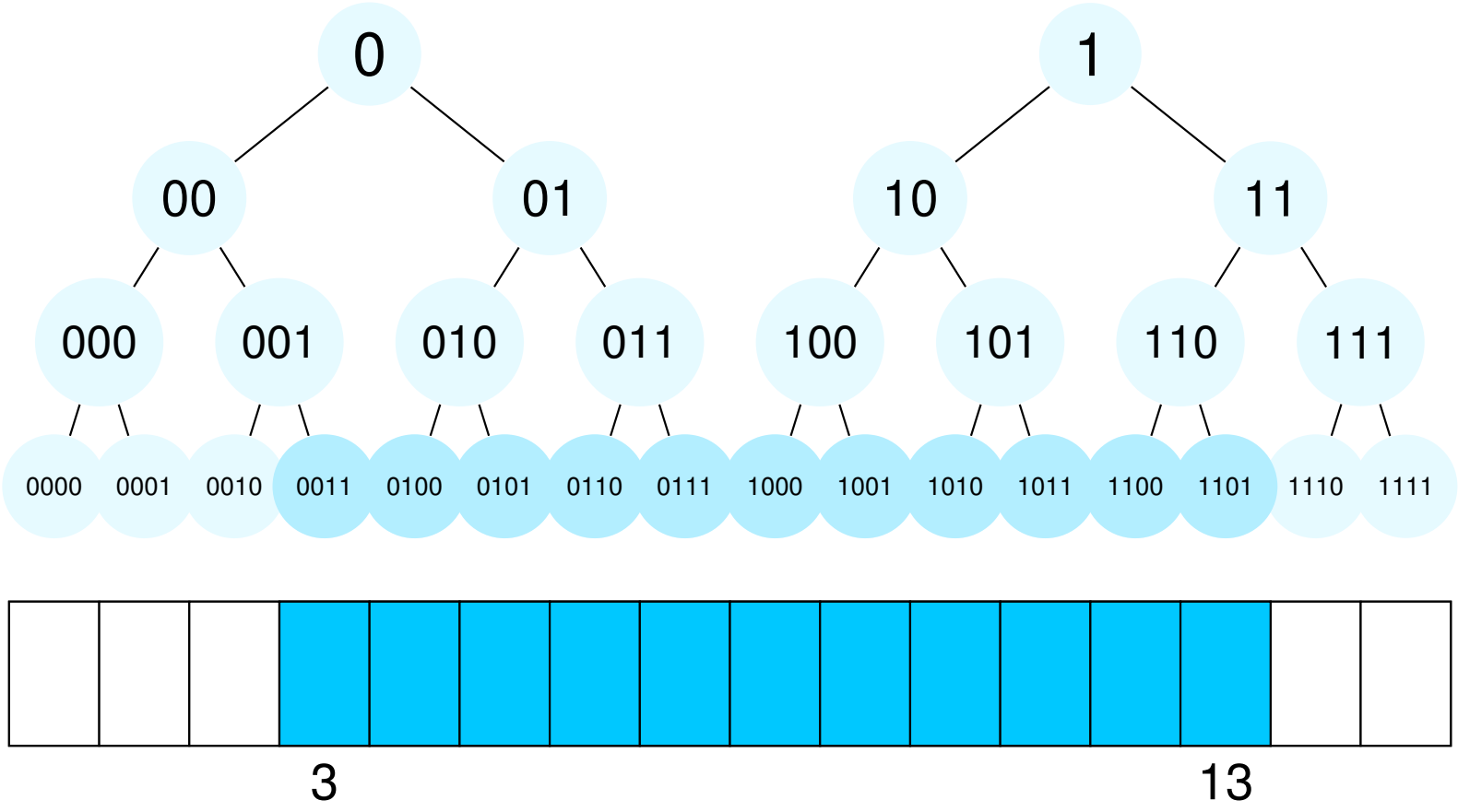
From Range to Vector

Query over $[0, 2^\ell - 1]$; example: $\ell = 4$, range $= [3, 13]$



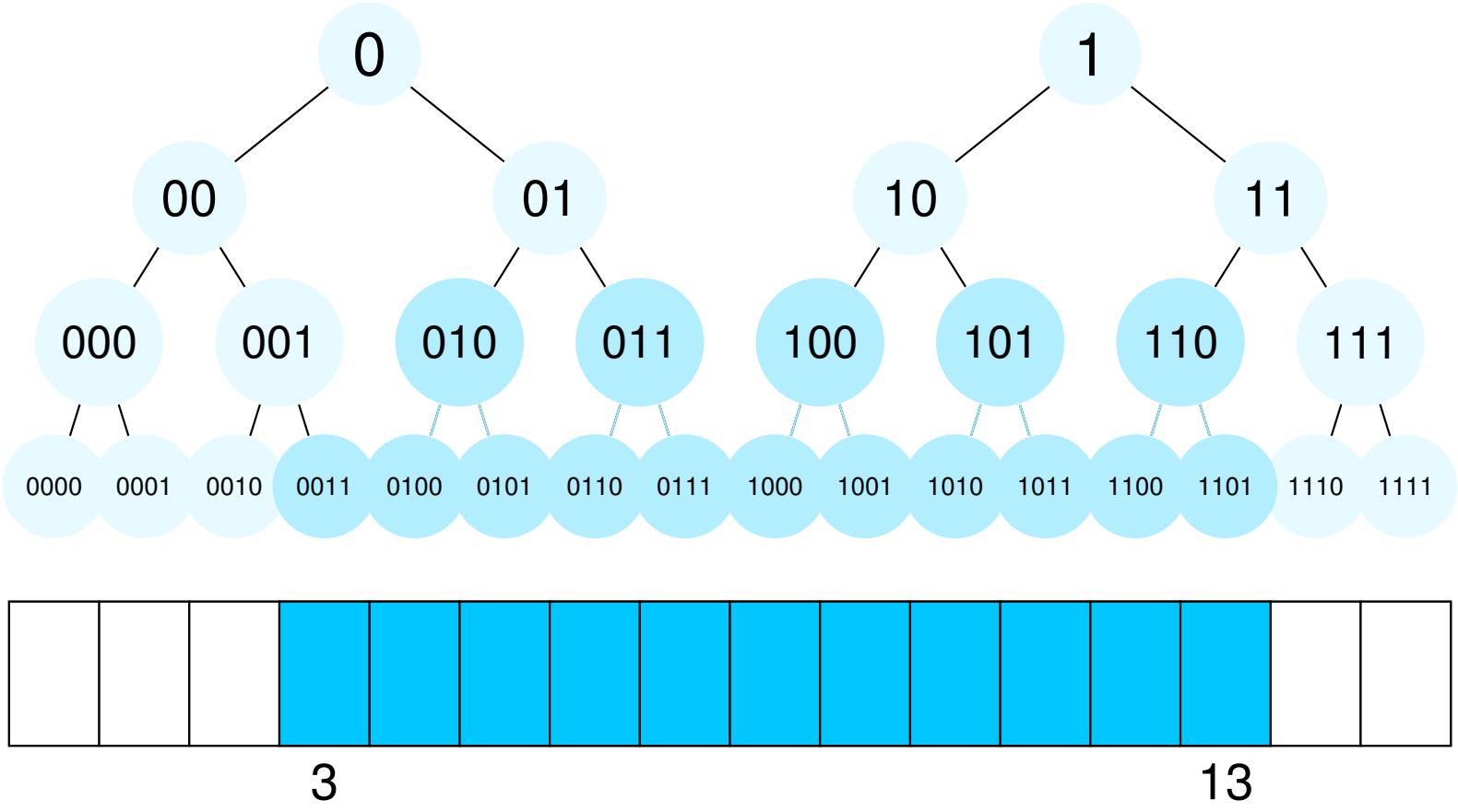
From Range to Vector

Query over $[0, 2^\ell - 1]$; example: $\ell = 4$, range $= [3, 13]$



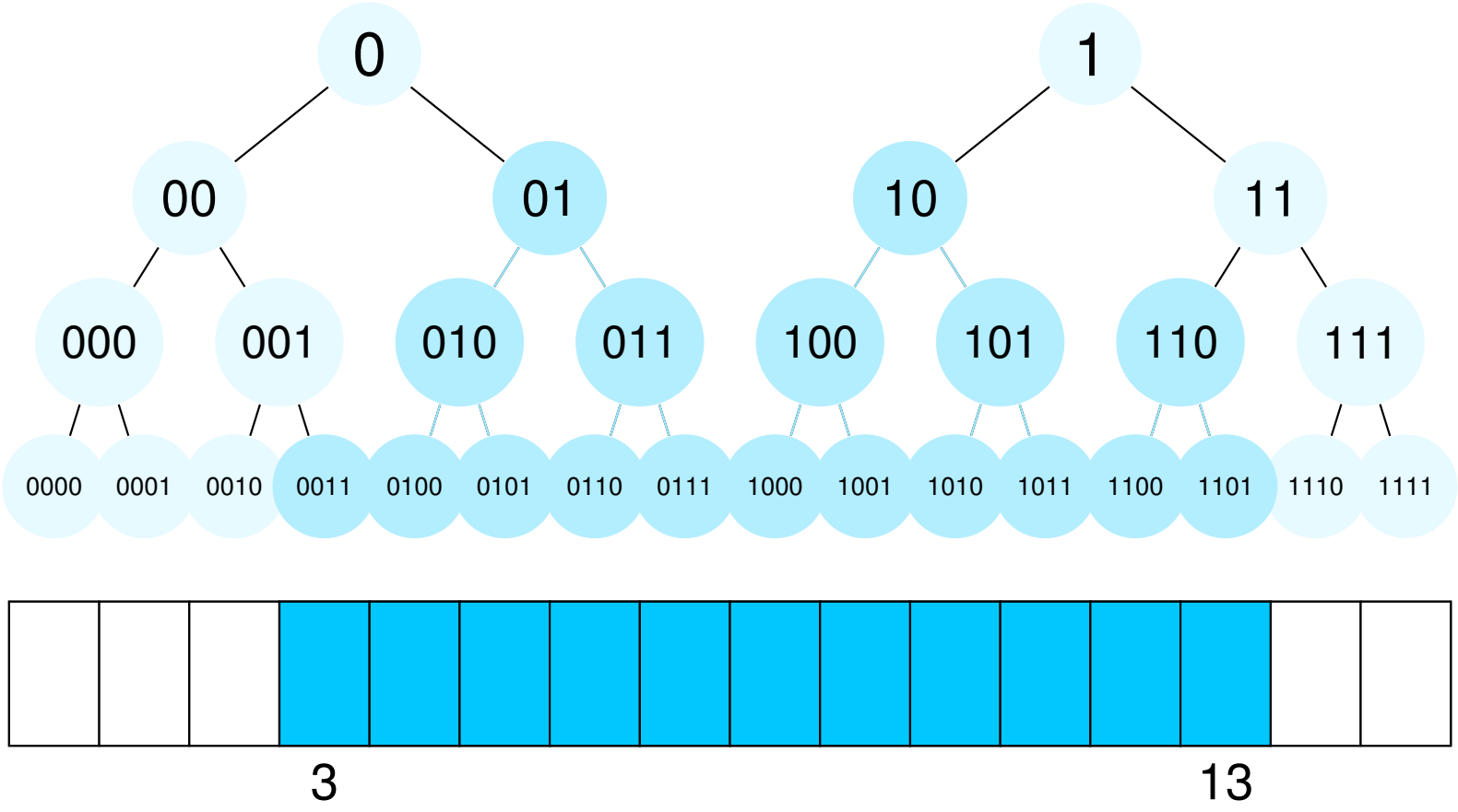
From Range to Vector

Query over $[0, 2^\ell - 1]$; example: $\ell = 4$, range $= [3, 13]$



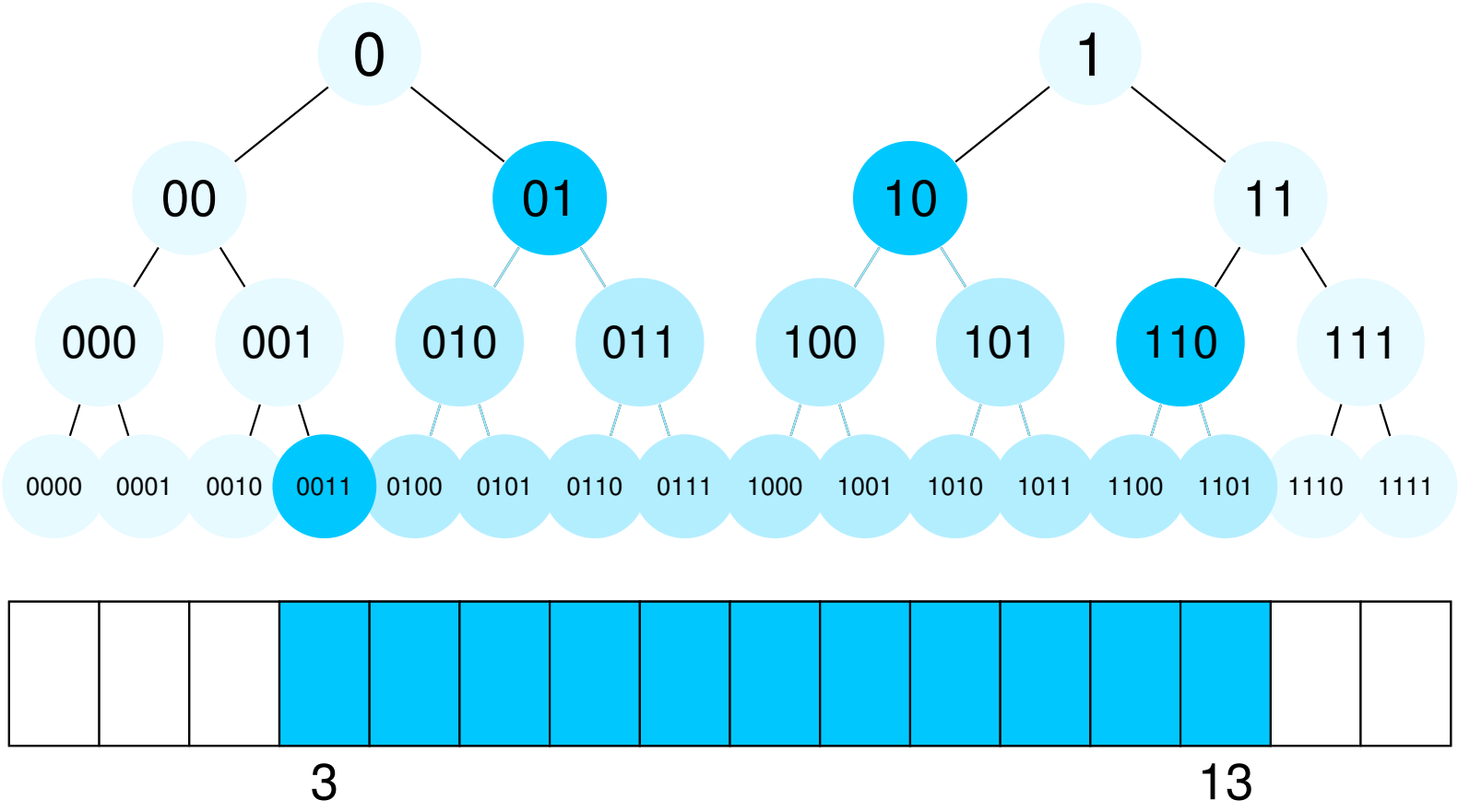
From Range to Vector

Query over $[0, 2^\ell - 1]$; example: $\ell = 4$, range $= [3, 13]$



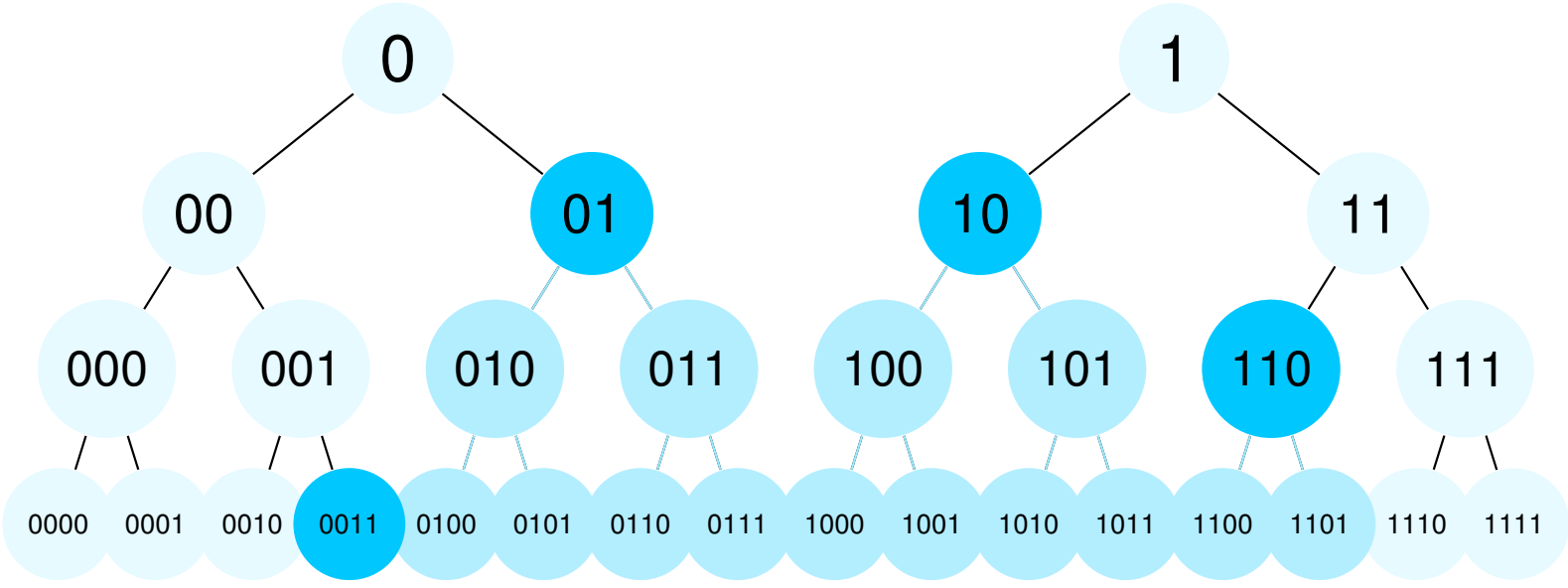
From Range to Vector

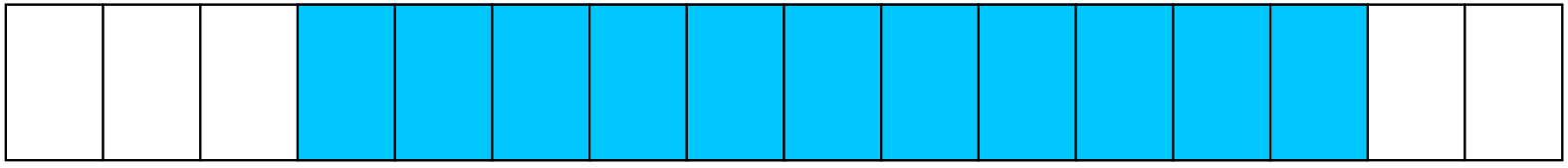
Query over $[0, 2^\ell - 1]$; example: $\ell = 4$, range $= [3, 13]$



From Range to Vector

Query over $[0, 2^\ell - 1]$; example: $\ell = 4$, range $= [3, 13]$





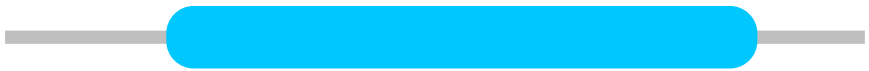
3 13

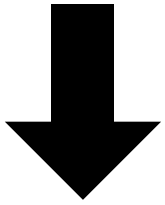
ε	ε	01	10	110	ε	0011	ε

From One-dimensional Range Query to Or Eq (2)

Range X

$X = [3, 13]$

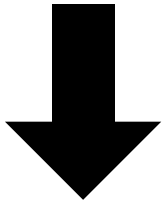




ε	ε	01	10	110	ε	0011	ε

Point Y

$Y = 8$



?	?	?	?	?	?	?	?

$$P_{\text{OR EQ}}(\mathbf{x}, \mathbf{y}) = ?$$

From Point to Vector

Point in $[0, 2^{\ell} - 1]$

From Point to Vector

Point in $[0, 2^\ell - 1]$; example: $\ell = 4$, point $= 8$

binary: 1000

From Point to Vector

Point in $[0, 2^\ell - 1]$; example: $\ell = 4$, point $= 8$

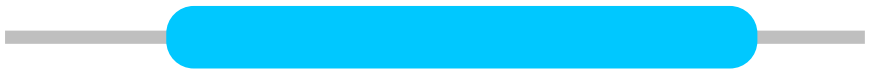
binary: 1000

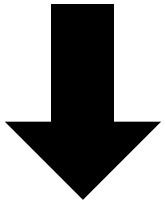
1	1	10	10	100	100	1000	1000

From One-dimensional Range Query to Or Eq (3)

Range X

$X = [3, 13]$

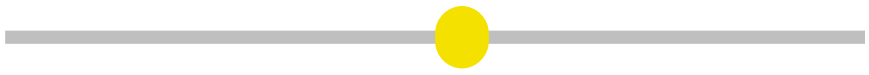


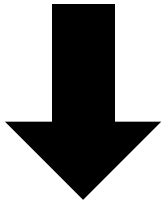


ε	ε	01	10	110	ε	0011	ε

Point Y

$Y = 8$





1	1	10	10	100	100	1000	1000

$P_{\text{OR EQ}}(X, Y) = ?$

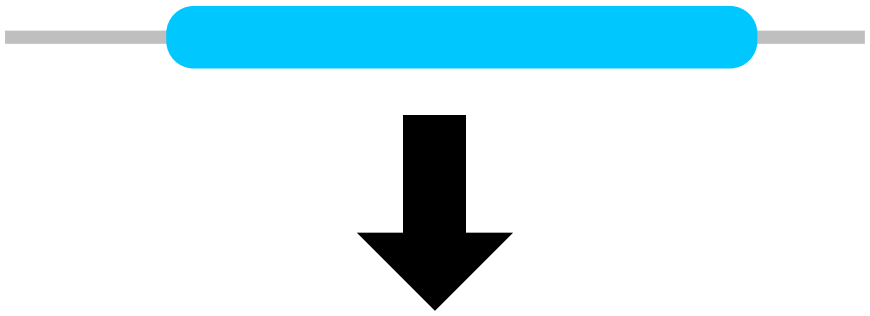
From One-dimensional Range Query to Or Eq (3)

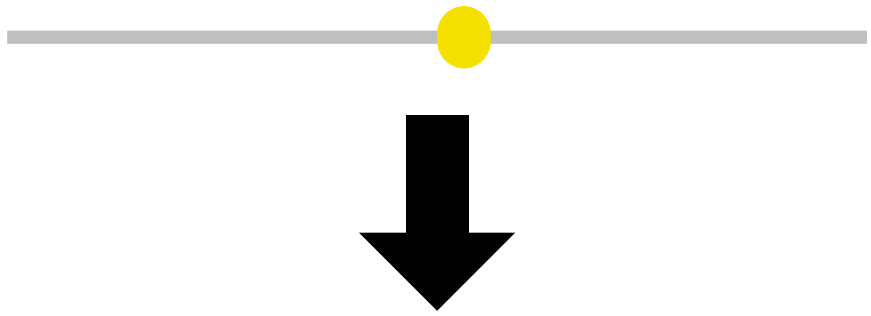
Range X

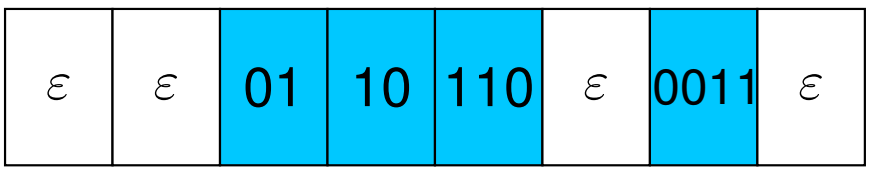
$X = [3, 13]$

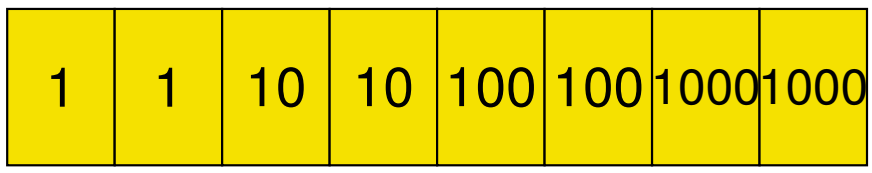
Point Y

$Y = 8$

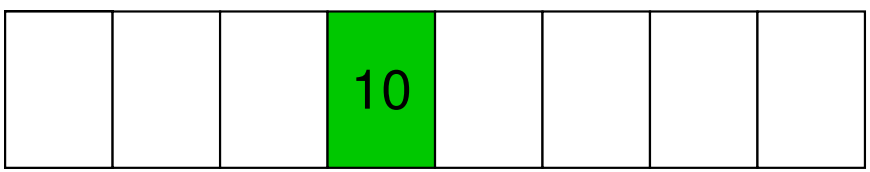








$P_{\text{OR EQ}}(X, Y) = 1$



One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$

Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

Or Eq predicate true iff:

$$\mathbf{x}_1 = \mathbf{y}_1 \quad \text{or} \quad \mathbf{x}_2 = \mathbf{y}_2 \quad \text{or} \quad \cdots \quad \text{or} \quad \mathbf{x}_\ell = \mathbf{y}_\ell$$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$

Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

MPK:

$$\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \cdots, \mathbf{A}_\ell, \mathbf{P}, \mathbf{G}$$

Or Eq predicate true iff:

$$\mathbf{x}_1 = \mathbf{y}_1 \quad \text{or} \quad \mathbf{x}_2 = \mathbf{y}_2 \quad \text{or} \quad \cdots \quad \text{or} \quad \mathbf{x}_\ell = \mathbf{y}_\ell$$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

$$\mathbf{A}|\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}|\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}|\cdots|\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}|\mathbf{P}$$

Or Eq predicate true iff:

$$\mathbf{x}_1 = \mathbf{y}_1 \quad \text{or} \quad \mathbf{x}_2 = \mathbf{y}_2 \quad \text{or} \quad \cdots \quad \text{or} \quad \mathbf{x}_\ell = \mathbf{y}_\ell$$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$

Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT:

LWE sample

$$\mathbf{A}|\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}|\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}|\cdots|\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}|\mathbf{P}$$

Or Eq predicate true iff:

$$\mathbf{x}_1 = \mathbf{y}_1 \quad \text{or} \quad \mathbf{x}_2 = \mathbf{y}_2 \quad \text{or} \quad \cdots \quad \text{or} \quad \mathbf{x}_\ell = \mathbf{y}_\ell$$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT: SK:

LWE sample

$\mathbf{A}|\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}|\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}|\cdots|\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}|\mathbf{P}$ $\quad \mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$

$\mathbf{U}_i$ s.t. $[\mathbf{A} \mid \mathbf{A}_i + \mathbf{y}_i\mathbf{G}]\, \mathbf{U}_i = \mathbf{P}$

Or Eq predicate true iff:

$\mathbf{x}_1 = \mathbf{y}_1 \quad \text{or} \quad \mathbf{x}_2 = \mathbf{y}_2 \quad \text{or} \quad \cdots \quad \text{or} \quad \mathbf{x}_\ell = \mathbf{y}_\ell$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT: SK:

LWE sample

$$\boxed{\mathbf{A}}\boxed{|\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}|}\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}|\cdots|\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}|\boxed{\mathbf{P}} \qquad \boxed{\mathbf{U}_1} \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$$

$\mathbf{U}_i$ s.t. $[\mathbf{A} \mid \mathbf{A}_i + \mathbf{y}_i\mathbf{G}]\,\mathbf{U}_i = \mathbf{P}$

Decryption if:

$$\mathbf{x}_1 = \mathbf{y}_1$$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT: SK:

LWE sample

$$\mathbf{A} \,|\, \mathbf{A}_1 + \mathbf{x}_1\mathbf{G} \,|\, \mathbf{A}_2 + \mathbf{x}_2\mathbf{G} \,|\, \cdots \,|\, \mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G} \,|\, \mathbf{P} \qquad \mathbf{U}_1 \;,\; \mathbf{U}_2 \;,\; \cdots \;,\; \mathbf{U}_\ell$$

$\mathbf{U}_i$ s.t. $[\mathbf{A} \mid \mathbf{A}_i + \mathbf{y}_i\mathbf{G}]\,\mathbf{U}_i = \mathbf{P}$

Decryption if:

$$\mathbf{x}_1 = \mathbf{y}_1$$

Attribute hiding property: Run over $1, \cdots, \ell$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT: SK:

LWE sample

$$\boxed{\mathbf{A}}\,|\,\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}\,|\,\boxed{\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}}\,|\cdots|\,\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}\,|\,\boxed{\mathbf{P}} \qquad \boxed{\mathbf{U}_1}\ ,\ \boxed{\mathbf{U}_2}\ ,\ \cdots\ ,\ \mathbf{U}_\ell$$

$\mathbf{U}_i$ s.t. $[\mathbf{A} \mid \mathbf{A}_i + \mathbf{y}_i\mathbf{G}]\,\mathbf{U}_i = \mathbf{P}$

Decryption if:

$$\mathbf{x}_2 = \mathbf{y}_2$$

Attribute hiding property: Run over $1, \cdots, \ell$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT: SK:

LWE sample

$$\boxed{\mathbf{A}}\boxed{\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}}\boxed{\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}}\cdots\boxed{\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}}\boxed{\mathbf{P}} \qquad \mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \boxed{\mathbf{U}_\ell}$$

$$\mathbf{U}_i \text{ s.t. } [\mathbf{A} \mid \mathbf{A}_i + \mathbf{y}_i\mathbf{G}]\, \mathbf{U}_i = \mathbf{P}$$

Decryption if:

$$\mathbf{x}_\ell = \mathbf{y}_\ell$$

Attribute hiding property: Run over $1, \cdots, \ell$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT: SK:

LWE sample

$$\boxed{\mathbf{A}}\boxed{\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}}|\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}|\cdots|\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}|\boxed{\mathbf{P}} \qquad \boxed{\mathbf{U}_1}, \mathbf{U}_2, \cdots, \mathbf{U}_\ell$$

$\mathbf{U}_i$ s.t. $[\mathbf{A} \mid \mathbf{A}_i + \mathbf{y}_i\mathbf{G}]\,\mathbf{U}_i = \mathbf{P}$

Decryption:

Correctness: which part ?

$\mathbf{x}_1 = \mathbf{y}_1$

redundant zeros in ENC $\Rightarrow$ DEC $\rightarrow (0, \cdots, 0, \mathbf{m})$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT: SK:

LWE sample

$$\boxed{\mathbf{A}}\boxed{\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}}\boxed{\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}}\cdots\boxed{\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}}\boxed{\mathbf{P}} \qquad \mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \boxed{\mathbf{U}_\ell}$$

$\mathbf{U}_i$ s.t. $[\mathbf{A} \mid \mathbf{A}_i + \mathbf{y}_i\mathbf{G}]\,\mathbf{U}_i = \mathbf{P}$

Decryption:

Correctness: which part ?

$\mathbf{x}_\ell \neq \mathbf{y}_\ell$

random value : $\mathsf{DEC} \rightarrow (0, 1, 1, \cdots, 1, 0)$

One-dimensional Scheme

Or Eq Predicate based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

Attribute: $\mathbf{x} \in \mathbb{Z}_q^\ell$ Predicate: $\mathbf{y} \in \mathbb{Z}_q^\ell$

CT: SK:

LWE sample

$\mathbf{A}|\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}|\mathbf{A}_2 + \mathbf{x}_2\mathbf{G}|\cdots|\mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}|\mathbf{P}$ $\mathbf{U}_1$, $\mathbf{U}_2$, $\cdots$, $\mathbf{U}_\ell$

$\mathbf{U}_i$ s.t. $[\mathbf{A} \mid \mathbf{A}_i + \mathbf{y}_i\mathbf{G}]\,\mathbf{U}_i = \mathbf{P}$

D-Dimensional set:

Use additive secret sharing [ABV12+]

Share $\mathbf{P}$ in $\mathbf{P}_1 + \mathbf{P}_2 + \cdots + \mathbf{P}_D$; $\mathbf{U}_i^j$ gives $\mathbf{P}_i$

Attribute-Hiding

$$\mathsf{CT} := \mathbf{s}^\top [\mathbf{A}, \mathbf{A}_1 + \mathbf{x}_1\mathbf{G}, \cdots, \mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}, \mathbf{P}] + [\mathbf{0}^\top, \cdots, \mathbf{0}^\top, \mathbf{b}'^\top \lfloor q/2 \rfloor] + \text{noise}$$

MPK CT

$\mathbf{A}, \mathbf{A}_1, \mathbf{G}$

$\mathbf{s}^\top \mathbf{A} + \text{noise}$

$\mathbf{s}^\top (\underbrace{\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}}_{\mathbf{A}'_1}) + \text{noise}$

Attribute-Hiding

$$\mathsf{CT} := \mathbf{s}^\top [\mathbf{A}, \mathbf{A}_1 + \mathbf{x}_1\mathbf{G}, \cdots, \mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}, \mathbf{P}] + [\mathbf{0}^\top, \cdots, \mathbf{0}^\top, \mathbf{b}'^\top \lfloor q/2 \rfloor] + \text{noise}$$

MPK CT

$\mathbf{A}, \mathbf{A}_1, \mathbf{G}$

$\mathbf{s}^\top \mathbf{A} + \text{noise}$

$\mathbf{s}^\top (\underbrace{\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}}_{\mathbf{A}'_1}) + \text{noise}$

$\equiv$

$\mathbf{A}, \mathbf{A}'_1 - \mathbf{x}_1\mathbf{G}, \mathbf{G}$

$\mathbf{s}^\top \mathbf{A} + \text{noise}$

$\mathbf{s}^\top \mathbf{A}'_1 + \text{noise}$

Attribute-Hiding

$$\mathsf{CT} := \mathbf{s}^\top [\mathbf{A}, \mathbf{A}_1 + \mathbf{x}_1\mathbf{G}, \cdots, \mathbf{A}_\ell + \mathbf{x}_\ell\mathbf{G}, \mathbf{P}] + [\mathbf{0}^\top, \cdots, \mathbf{0}^\top, \mathbf{b}'^\top \lfloor q/2 \rfloor] + \text{noise}$$

MPK CT

$\mathbf{A}, \mathbf{A}_1, \mathbf{G}$		$\mathbf{A}, \mathbf{A}'_1 - \mathbf{x}_1\mathbf{G}, \mathbf{G}$		$\mathbf{A}, \mathbf{A}'_1 - \mathbf{x}_1\mathbf{G}, \mathbf{G}$
$\mathbf{s}^\top\mathbf{A} + \text{noise}$		$\mathbf{s}^\top\mathbf{A} + \text{noise}$		random
$\mathbf{s}^\top (\underbrace{\mathbf{A}_1 + \mathbf{x}_1\mathbf{G}}_{\mathbf{A}'_1}) + \text{noise}$	$\equiv$	$\mathbf{s}^\top\mathbf{A}'_1 + \text{noise}$	$\approx$ LWE	random

Summary

Lattice-based predicate encryption scheme for multi-dimensional range queries

Reference	Size		Time		Attribute hiding	based on
	PK and CT	SK	ENC	DEC		
[BW07] (KP)	$O(D \cdot T)$	$O(D)$	$O(D \cdot T)$	$O(D)$	fully	pairings
[SBCSP07](KP,CP)	$O(D \log T)$	$O(D \log T)$	$O(D \log T)$	$O((\log T)^D)$	weakly	pairings
This paper (KP,CP)	$O(D \log T)$	$O(D \log T)$	$O(D \log T)$	$O((\log T)^D)$	weakly	lattices

Summary

Lattice-based predicate encryption scheme for multi-dimensional range queries

Reference	Size		Time		Attribute hiding	based on
	PK and CT	SK	ENC	DEC		
[BW07] (KP)	$O(D \cdot T)$	$O(D)$	$O(D \cdot T)$	$O(D)$	fully	pairings
[SBCSP07](KP,CP)	$O(D \log T)$	$O(D \log T)$	$O(D \log T)$	$O((\log T)^D)$	weakly	pairings
This paper (KP,CP)	$O(D \log T)$	$O(D \log T)$	$O(D \log T)$	$O((\log T)^D)$	weakly	lattices

Open questions

Summary

Lattice-based predicate encryption scheme for multi-dimensional range queries

Reference	Size		Time		Attribute hiding	based on
	PK and CT	SK	ENC	DEC		
[BW07] (KP)	$O(D \cdot T)$	$O(D)$	$O(D \cdot T)$	$O(D)$	fully	pairings
[SBCSP07](KP,CP)	$O(D \log T)$	$O(D \log T)$	$O(D \log T)$	$O((\log T)^D)$	weakly	pairings
This paper (KP,CP)	$O(D \log T)$	$O(D \log T)$	$O(D \log T)$	$O((\log T)^D)$	weakly	lattices

Open questions

Thanks!