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
Tuesday, March 31

Online Dating Configuration

Profile

Alice
Header
Hobbies
Pictures

Online Dating Configuration

Profile	Preferences	
Alice	N pictures:	$x_1 > 0$
Header	Children:	$x_2 = 0$
Hobbies	Age:	$24 \leq x_3 \leq 36$
Pictures	Salary:	$\$\$\$\$ \leq x_4 \leq \max$

Online Dating Configuration

Profile	Preferences	
Alice Header Hobbies Pictures	N pictures:	$x_1 > 0$
	Children:	$x_2 = 0$
	Age:	$24 \leq x_3 \leq 36$
	Salary:	$\$\$\$\$ \leq x_4 \leq \max$

Online dating using Attribute-Based Encryption [GVW13, BGG+14]

Online Dating Configuration

Profile	Preferences	
Alice	N pictures:	$? \leq x_1 \leq ?$
Header	Children:	$? \leq x_2 \leq ?$
Hobbies	Age:	$? \leq x_3 \leq ?$
Pictures	Salary:	$? \leq x_4 \leq ?$

ABE does not ensure attribute hiding

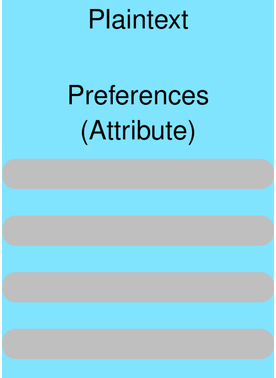
Online Dating Configuration

Profile	Preferences	
Alice	N pictures:	$? \leq x_1 \leq ?$
Header	Children:	$? \leq x_2 \leq ?$
Hobbies	Age:	$? \leq x_3 \leq ?$
Pictures	Salary:	$? \leq x_4 \leq ?$

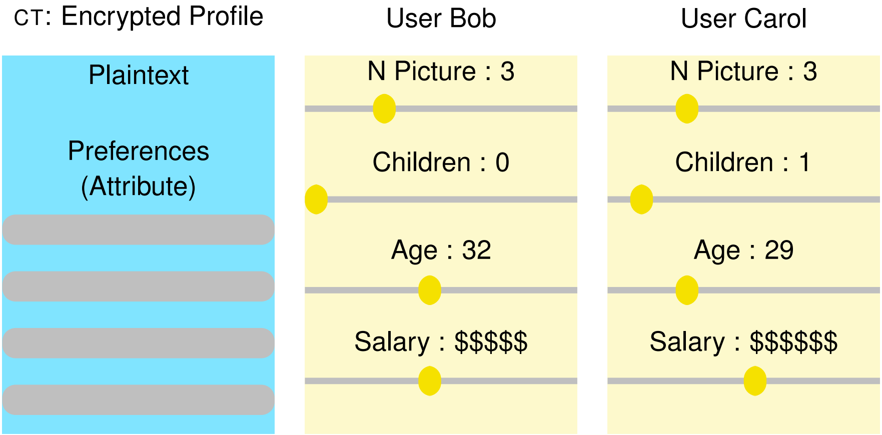
Online dating using Predicate Encryption [BW07, SBC+07,KSW08]

Online Dating Encryption Scheme

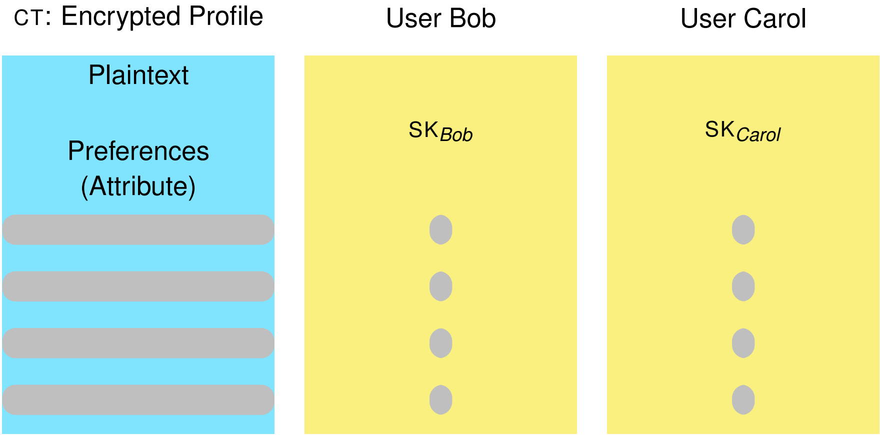
CT: Encrypted Profile



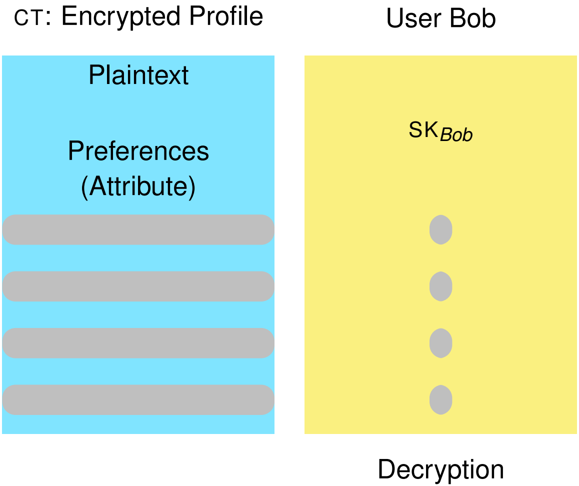
Online Dating Encryption Scheme



Online Dating Encryption Scheme



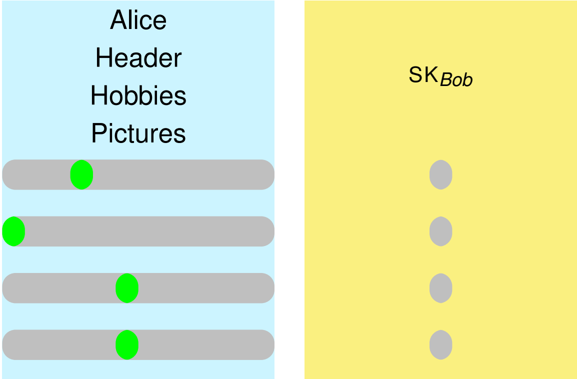
Online Dating Encryption Scheme



Online Dating Encryption Scheme

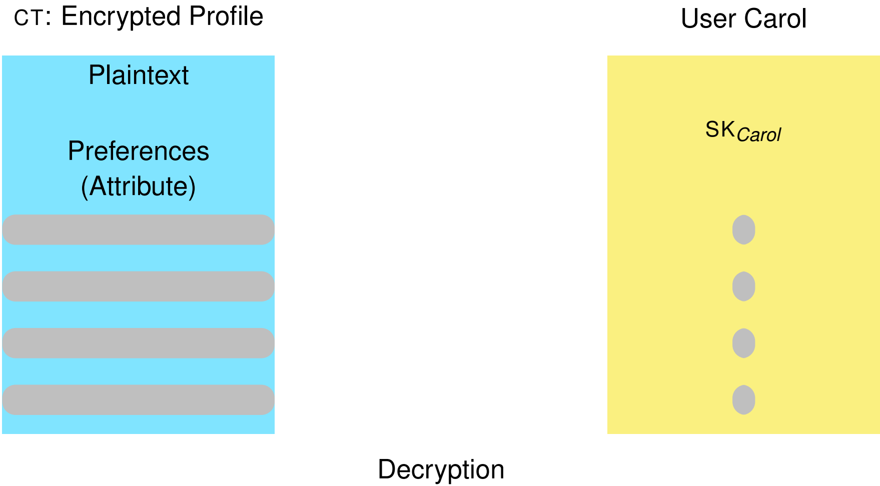
m : Decrypted Profile

User Bob



Successful decryption and learning the matches

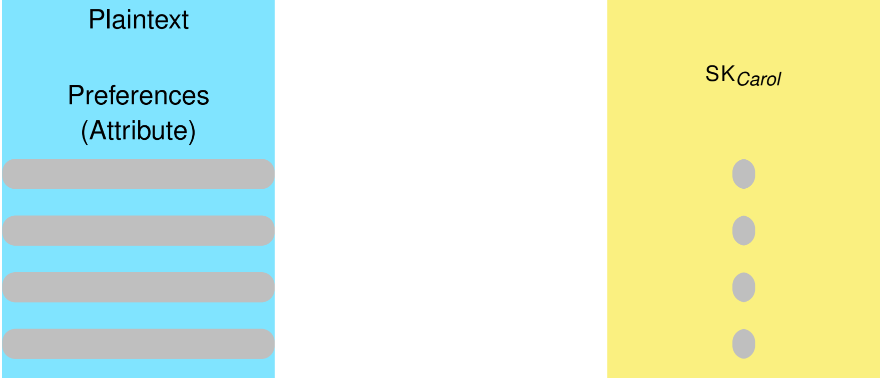
Online Dating Encryption Scheme



Online Dating Encryption Scheme

CT: Encrypted Profile

User Carol



Incorrect decryption, no more information

Result

Theorem

Predicate Encryption

for

MDRQ

from

LWE

Prior works

from pairings

[BW07,SBC+07]

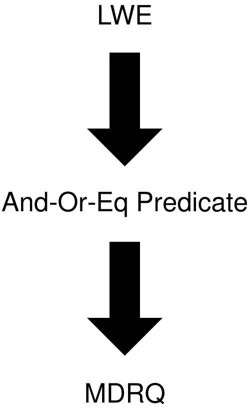
Result

Theorem

Predicate Encryption
for
MDRQ
from
LWE

Prior works

from pairings
[BW07,SBC+07]



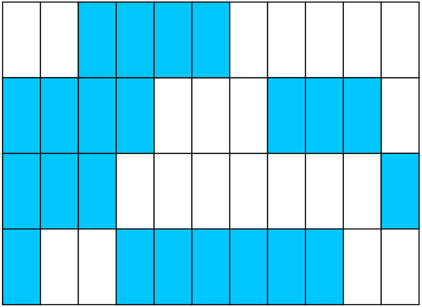
And Or Eq Predicate

Disjunction of conjunction of equality queries

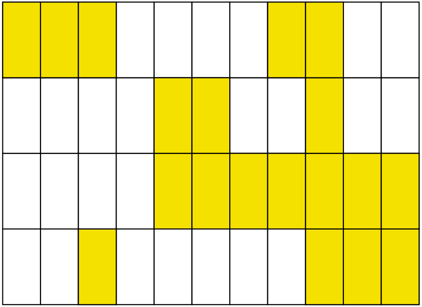
$P_{\text{AND-OR-EQ}} : \mathbb{Z}_q^{D\times\ell} \times \mathbb{Z}_q^{D\times\ell} \to \{0,1\}$

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

Matrix X



Matrix Y



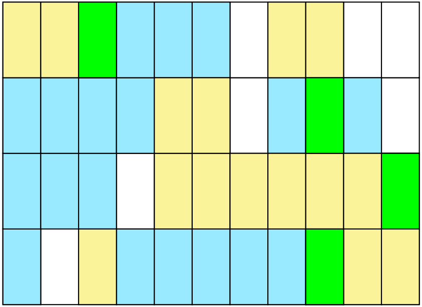
And Or Eq Predicate

Disjunction of conjunction of equality queries

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

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

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



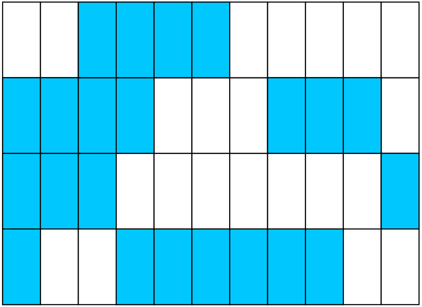
And Or Eq Predicate

Disjunction of conjunction of equality queries

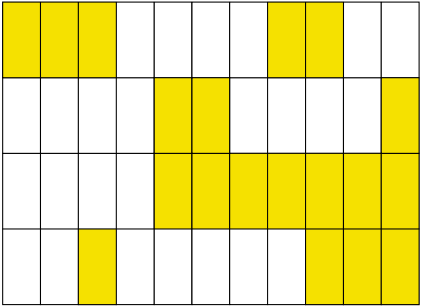
$\mathrm{P}_{\text{AND-OR-EQ}} : \mathbb{Z}_q^{D \times \ell} \times \mathbb{Z}_q^{D \times \ell} \to \{0, 1\}$

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

Matrix X



Matrix Y'



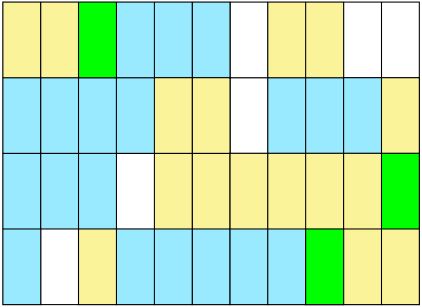
And Or Eq Predicate

Disjunction of conjunction of equality queries

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

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

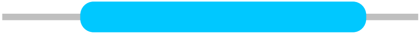
$$\mathsf{P}_{\text{AND-OR-EQ}}(X, Y') = 0$$



From Range Query to And Or Eq

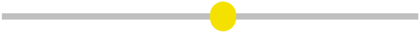
Range X

$X = [3, 13]$



Point Y

$Y = 8$



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

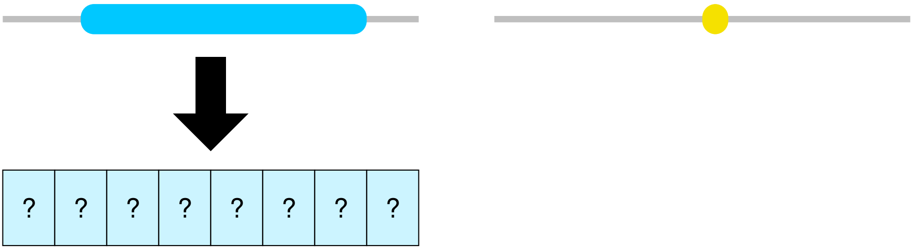
From Range Query to And Or Eq

Range X

$X = [3, 13]$

Point Y

$Y = 8$

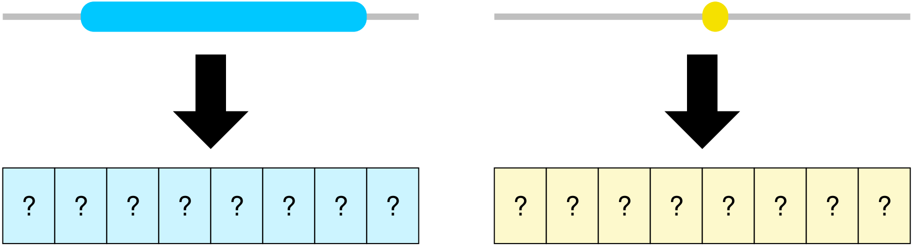


$$P_{\text{AND OR EQ}}(X, Y) = ?$$

From Range Query to And Or Eq

Range X — Point Y

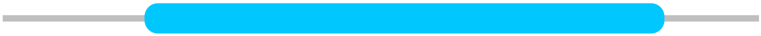
$X = [3, 13]$ — $Y = 8$



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

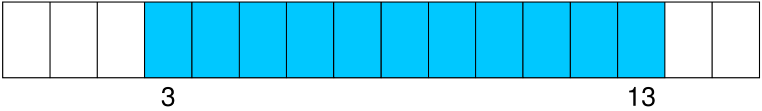
From Range to Vector

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



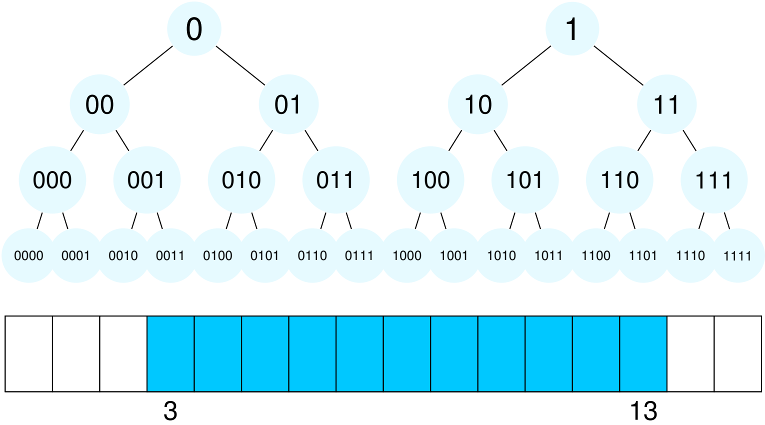
From Range to Vector

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



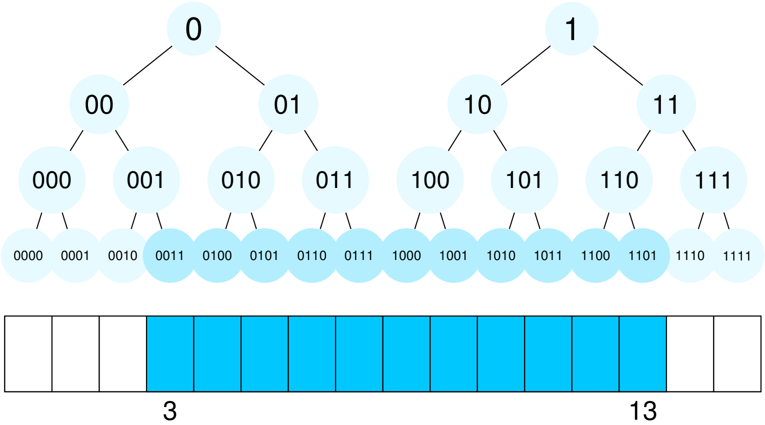
From Range to Vector

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



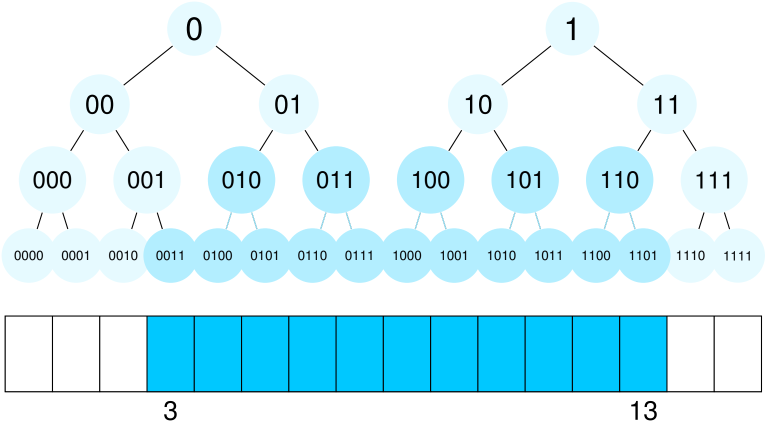
From Range to Vector

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



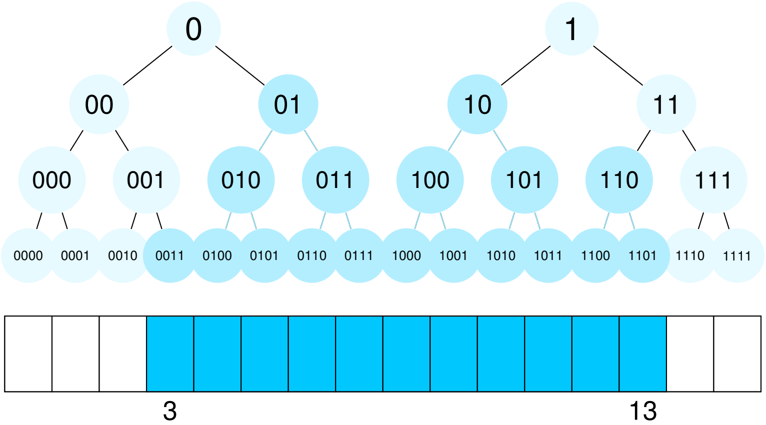
From Range to Vector

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



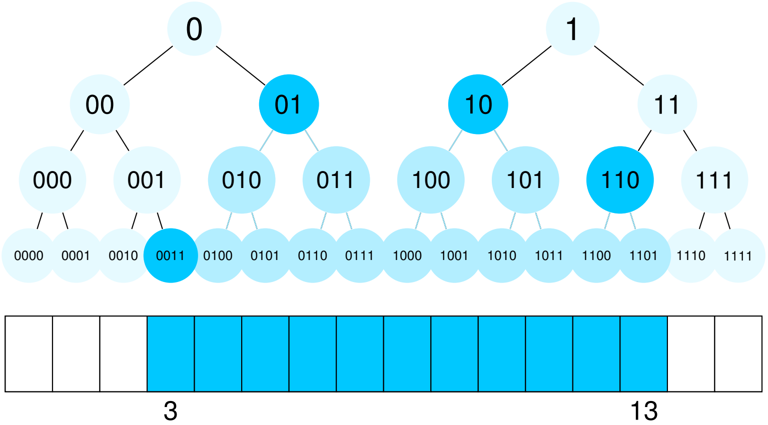
From Range to Vector

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



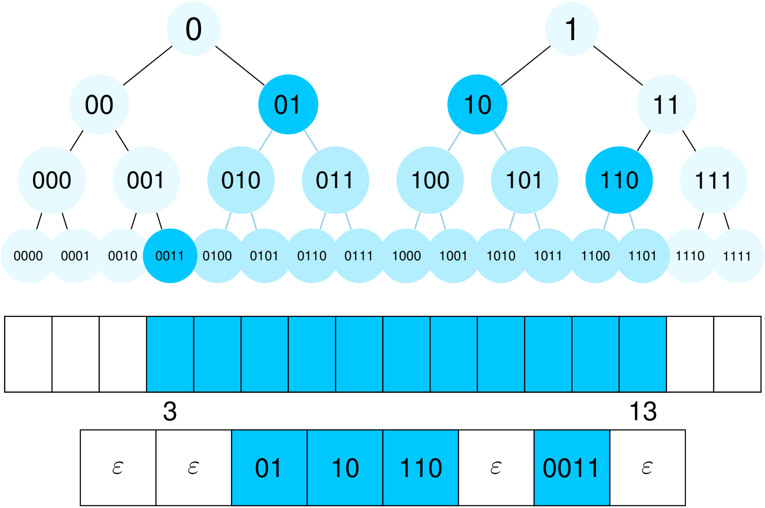
From Range to Vector

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 $= [3, 13]$



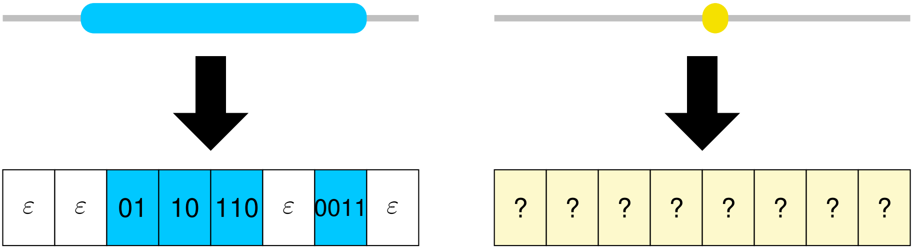
From Range Query to And Or Eq (2)

Range X

$X = [3, 13]$

Point Y

$Y = 8$



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

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

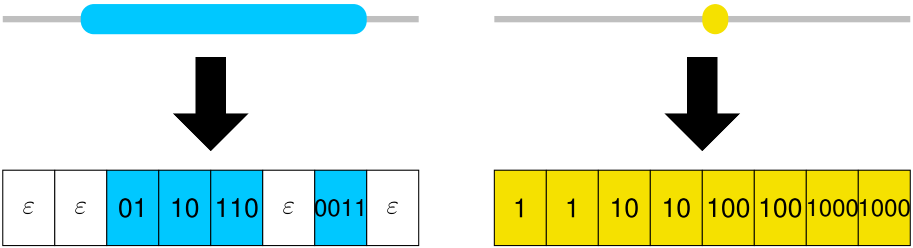
From Range Query to And Or Eq (3)

Range X

$X = [3, 13]$

Point Y

$Y = 8$



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

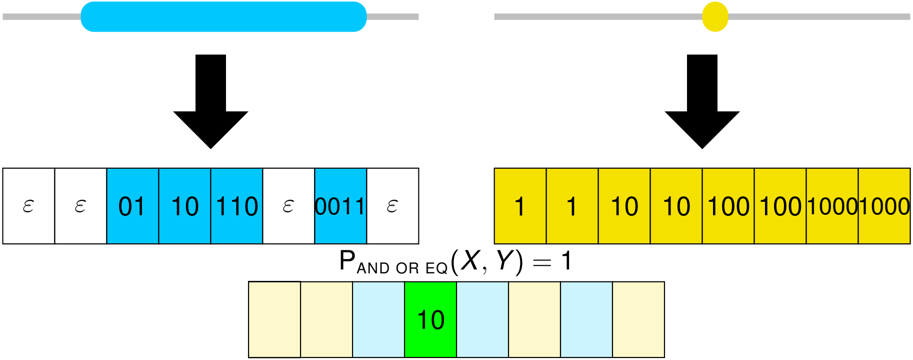
From Range Query to And Or Eq (3)

Range X

$X = [3, 13]$

Point Y

$Y = 8$



One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

MPK:

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

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

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

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

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

SK:

$$\mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$$

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

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

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

SK:

$\mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$

$\mathbf{U}_i$ 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

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

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

SK:

$\mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$

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

Decryption:

Attribute hiding property

Run over $1, \cdots, \ell$

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

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

SK:

$$\mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$$

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

Decryption:

Attribute hiding property

Run over $1, \cdots, \ell$

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

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

SK:

$\mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$

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

Decryption:

Attribute hiding property

Run over $1, \cdots, \ell$

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

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

SK:

$\mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$

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

Decryption:

Correctness: which part ?

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

redondants zeros : DEC$\rightarrow$ $(0, \cdots, 0, \mathbf{m})$

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

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

SK:

$\mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$

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

Decryption:

Correctness: which part ?

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

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

One-dimensional Scheme

MDRQ based on standard LWE

Predicate Encryption scheme using anonymous IBE [ABB10,CHKP10]

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

CT:

LWE sample

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

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

SK:

$\mathbf{U}_1 \quad , \quad \mathbf{U}_2 \quad , \quad \cdots \quad , \quad \mathbf{U}_\ell$

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

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

$\mathsf{CT} := \mathbf{s}^\top[\mathbf{A}, \mathbf{A}_1 + x_1\mathbf{G}, \cdots, \mathbf{A}_\ell + x_\ell\mathbf{G}, \mathbf{P}] + [\mathbf{0}^\top, \cdots, \mathbf{0}^\top, \mathbf{b}'^\top\lfloor q/2 \rfloor]$ + noise

MPK CT

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

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

$\mathbf{s}^\top \underbrace{(\mathbf{A}_1 + x_1\mathbf{G})}_{\mathbf{A}'_1}$ + noise

Attribute-Hiding

$$\mathsf{CT} := \mathbf{s}^\top[\mathbf{A}, \mathbf{A}_1 + x_1\mathbf{G}, \cdots, \mathbf{A}_\ell + x_\ell\mathbf{G}, \mathbf{P}] + [\mathbf{0}^\top, \cdots, \mathbf{0}^\top, \mathbf{b}'^\top\lfloor q/2 \rfloor] + \text{noise}$$

MPK CT

$\mathbf{A}, \mathbf{A}_1, \mathbf{G}$ | $\mathbf{A}, \mathbf{A}_1' - x_1\mathbf{G}, \mathbf{G}$

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

$\mathbf{s}^\top \underbrace{(\mathbf{A}_1 + x_1\mathbf{G})}_{\mathbf{A}_1'}$ + noise $\equiv$ $\mathbf{s}^\top\mathbf{A}_1'$ + noise

Attribute-Hiding

$\mathsf{CT} := \mathbf{s}^\top[\mathbf{A}, \mathbf{A}_1 + x_1\mathbf{G}, \cdots, \mathbf{A}_\ell + x_\ell\mathbf{G}, \mathbf{P}] + [\mathbf{0}^\top, \cdots, \mathbf{0}^\top, \mathbf{b}'^\top\lfloor q/2 \rfloor] + \text{noise}$

MPK CT

$\mathbf{A}, \mathbf{A}_1, \mathbf{G}$		$\mathbf{A}, \mathbf{A}'_1 - x_1\mathbf{G}, \mathbf{G}$		$\mathbf{A}, \mathbf{A}'_1 - x_1\mathbf{G}, \mathbf{G}$
$\mathbf{s}^\top\mathbf{A}$ + noise		$\mathbf{s}^\top\mathbf{A}$ + noise		random
$\mathbf{s}^\top \underbrace{(\mathbf{A}_1 + x_1\mathbf{G})}_{\mathbf{A}'_1}$ + noise	$\equiv$	$\mathbf{s}^\top\mathbf{A}'_1$ + noise	$\approx$ LWE	random

Summary

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

Selectively secure, weakly attribute hiding

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 query

Selectively secure, weakly attribute hiding

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

Thanks for your attention !