FastGeo: Efficient Geometric Range Queries on Encrypted Spatial Data

TDSC2019

Boyang Wang, Student Member, IEEE, Ming Li, Member, IEEE, and Li Xiong, Member, IEEE

I. Introduction

I. Introduction

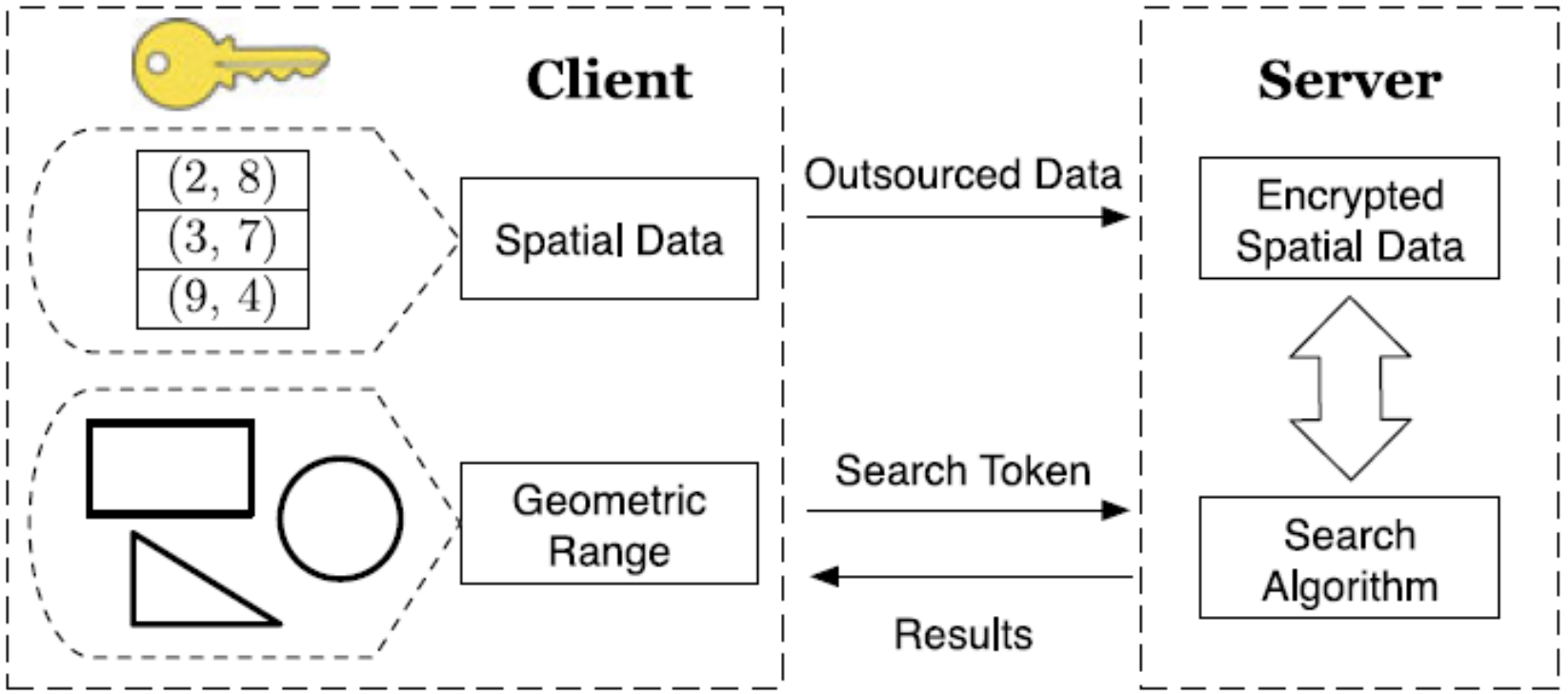
- Searchable Encryption
  - Data
  - Sql queries
    - Keyword search -- comparison
    - Range search -- comparison

I. Introduction

- Searchable Encryption
  - Data
  - Sql queries
    - Keyword search -- comparison
    - Range search -- comparison

- Searchable Encryption
  - Spatial data
  - Arbitrary geometric range queries
    - Circles range queries -- compute-then-compare

II. Problem



- Server is honest-but-curious

II. Problem

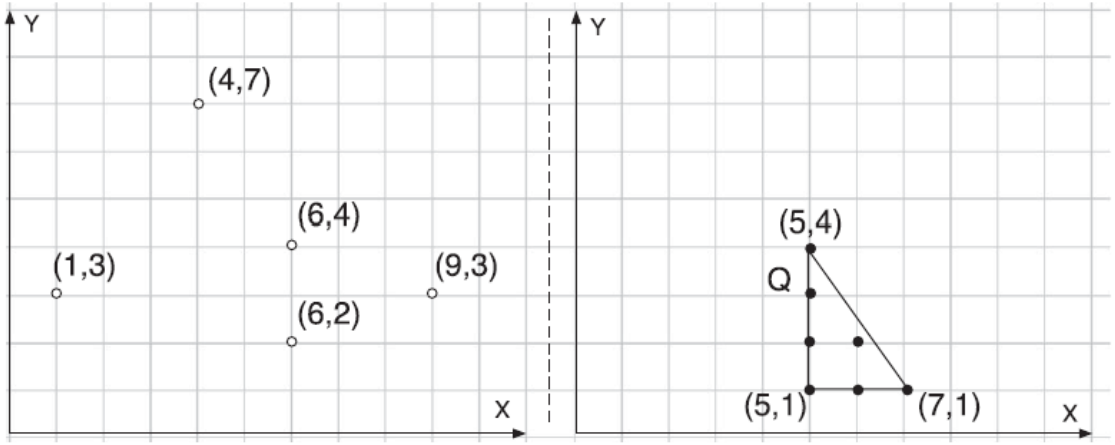
- **Geometrically Searchable Encryption(GSE)**
  - sk ← GenKey(λ)
  - **Γ** ← BuildIndex(**Đ**, m)
  - **Γ*** ← Enc(**Γ**, sk)
  - tk_Q ← GenToken(Q, sk, m)
  - $\boldsymbol{I}_Q$ ← Query(**Γ***, tk_Q)

III. FastGeo: An Efficient GSE

- **Two-level search**
  - First level relies on equality checking.
  - Second level depends on evaluating inner products.

III. FastGeo: An Efficient GSE

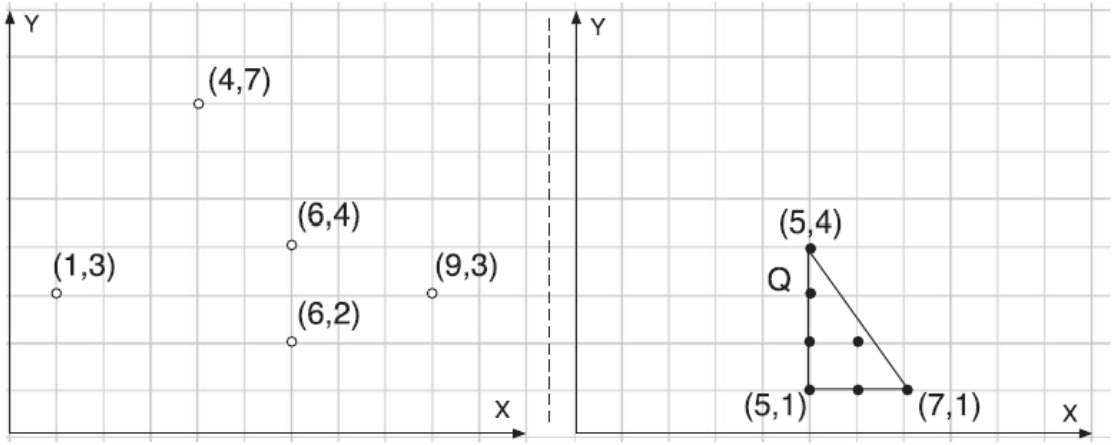
Transform data and queries to equality-vector form.



$x \in [0,9]$ *and* $y \in [0,9]$ only integers

III. FastGeo: An Efficient GSE

Transform data and queries to equality-vector form.

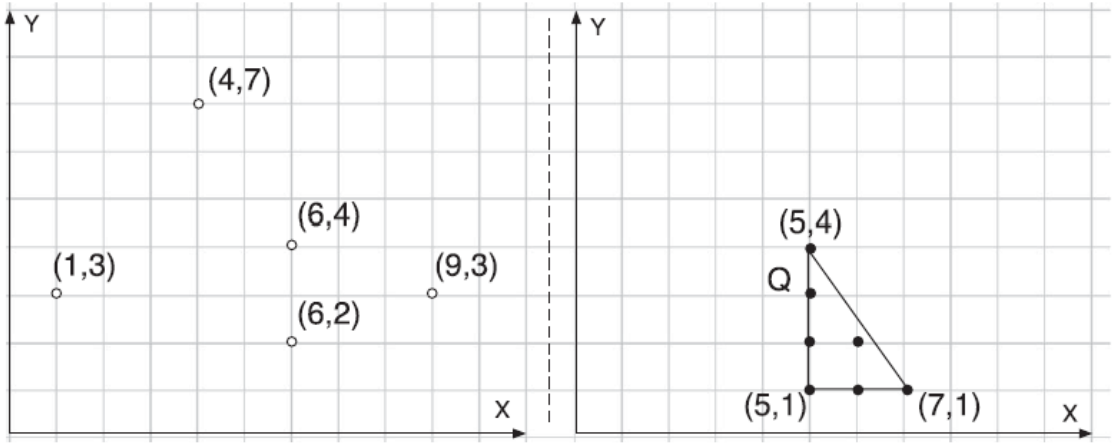


$x \in [0,9]$ *and* $y \in [0,9]$ only integers

Dictionary	Link Lists
$x = 1$	$\rightarrow (0,0,0,1,0,0,0,0,0,0)$
$x = 4$	$\rightarrow (0,0,0,0,0,0,0,1,0,0)$
$x = 6$	$\rightarrow (0,0,1,0,0,0,0,0,0,0) \rightarrow (0,0,0,0,1,0,0,0,0,0)$
$x = 9$	$\rightarrow (0,0,0,1,0,0,0,0,0,0)$

III. FastGeo: An Efficient GSE

Transform data and queries to equality-vector form.



$x \in [0,9]$ *and* $y \in [0,9]$ only integers

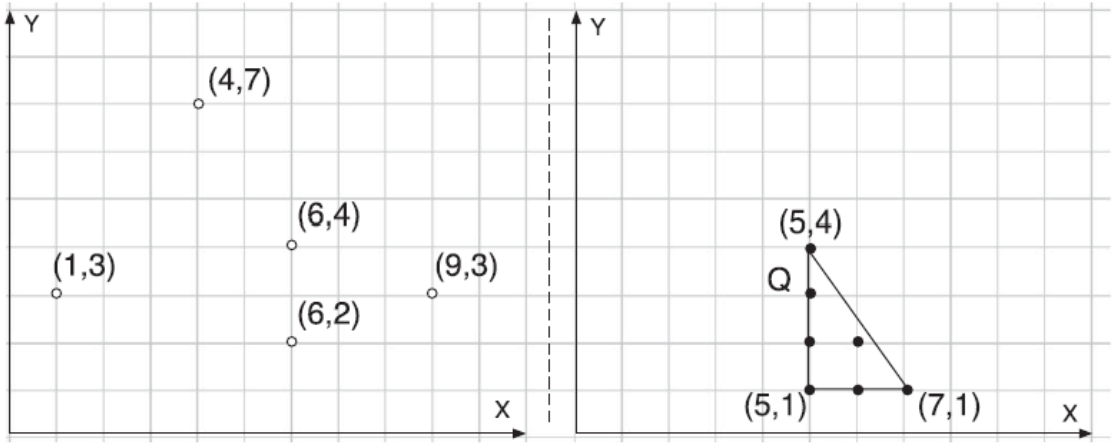
Dictionary	Link Lists
$x = 1$	$\rightarrow (0,0,0,1,0,0,0,0,0,0)$
$x = 4$	$\rightarrow (0,0,0,0,0,0,0,1,0,0)$
$x = 6$	$\rightarrow (0,0,1,0,0,0,0,0,0,0) \rightarrow (0,0,0,0,1,0,0,0,0,0)$
$x = 9$	$\rightarrow (0,0,0,1,0,0,0,0,0,0)$

Possible Points inside Query Q

$(5,1), (5,2), (5,3), (5,4)$
$(6,1), (6,2)$
$(7,1)$

III. FastGeo: An Efficient GSE

Transform data and queries to equality-vector form.



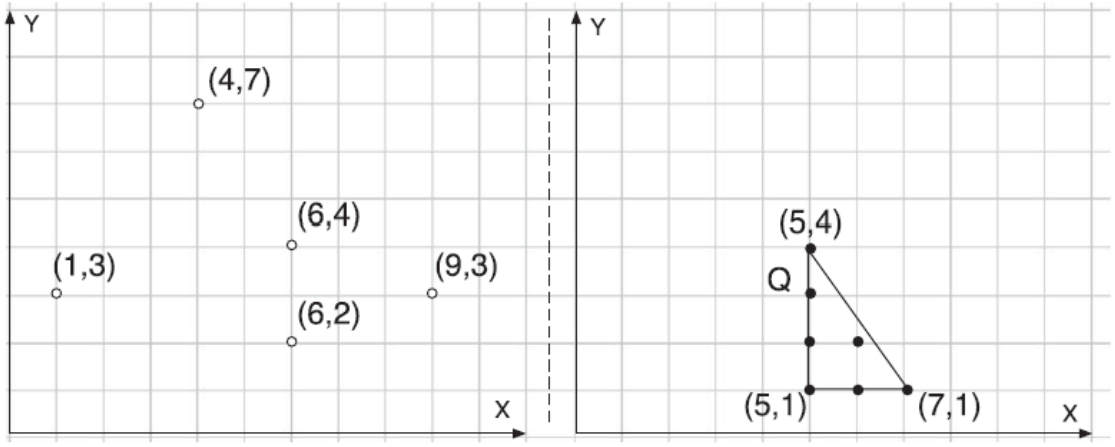
$x \in [0,9]$ *and* $y \in [0,9]$ only integers

Dictionary	Link Lists
$x = 1$	$\rightarrow (0,0,0,1,0,0,0,0,0,0)$
$x = 4$	$\rightarrow (0,0,0,0,0,0,0,1,0,0)$
$x = 6$	$\rightarrow (0,0,1,0,0,0,0,0,0,0) \rightarrow (0,0,0,0,1,0,0,0,0,0)$
$x = 9$	$\rightarrow (0,0,0,1,0,0,0,0,0,0)$

x-subqueries	y-subqueries
$x = 5$	$(1,0,0,0,0,1,1,1,1,1)$
$x = 6$	$(1,0,0,1,1,1,1,1,1,1)$
$x = 7$	$(1,0,1,1,1,1,1,1,1,1)$

III. FastGeo: An Efficient GSE

Search with equality-vector form.



$x \in [0,9]$ *and* $y \in [0,9]$ only integers

1. Equality checking
2. Evaluate an inner product

$$
\begin{aligned}
&x = 5 \text{ false} \\
&x = 6 \text{ true} \\
&\quad < (0,0,1,0,0,0,0,0,0,0), (1,0,0,1,1,1,1,1,1,1) >= 0 \\
&\quad < (0,0,0,0,1,0,0,0,0,0), (1,0,0,1,1,1,1,1,1,1) >= 1 \neq 0 \\
&x = 7 \text{ false}
\end{aligned}
$$

III. FastGeo: An Efficient GSE

Search with enhanced equality-vector form.

Client give a search token $tk_Q = \{\{[x_1], [\overrightarrow{v_1}]\}, \{[x_2], [\overrightarrow{v_2}]\}\}$

Server mismatch it as $tk_{Q'} = \{\{[x_1], [\overrightarrow{v_2}]\}, \{[x_2], [\overrightarrow{v_1}]\}\}$

III. FastGeo: An Efficient GSE

Search with enhanced equality-vector form.

Client give a search token $tk_Q = \{\{[x_1], [\overrightarrow{v_1}]\}, \{[x_2], [\overrightarrow{v_2}]\}\}$

Server mismatch it as $tk_{Q'} = \{\{[x_1], [\overrightarrow{v_2}]\}, \{[x_2], [\overrightarrow{v_1}]\}\}$

For data point (6, 2), its y-value in enhanced vector form is

$$\overrightarrow{u_e} = (0,0, H(6), 0, 0, 0, 0, 0, 0, 0, -1)$$

For x-subquery x=6 and its y-subquery $y \in [1,2]$, its y-subquery is

$$\overrightarrow{v_e} = (0, 1,1,0, 0, 0, 0, 0, 0, 0, H(6))$$

IV. Evaluation

A real-world spatial dataset contains 49870 tuples.

Main parameters:

- Vector length m
- First-level query size q_1

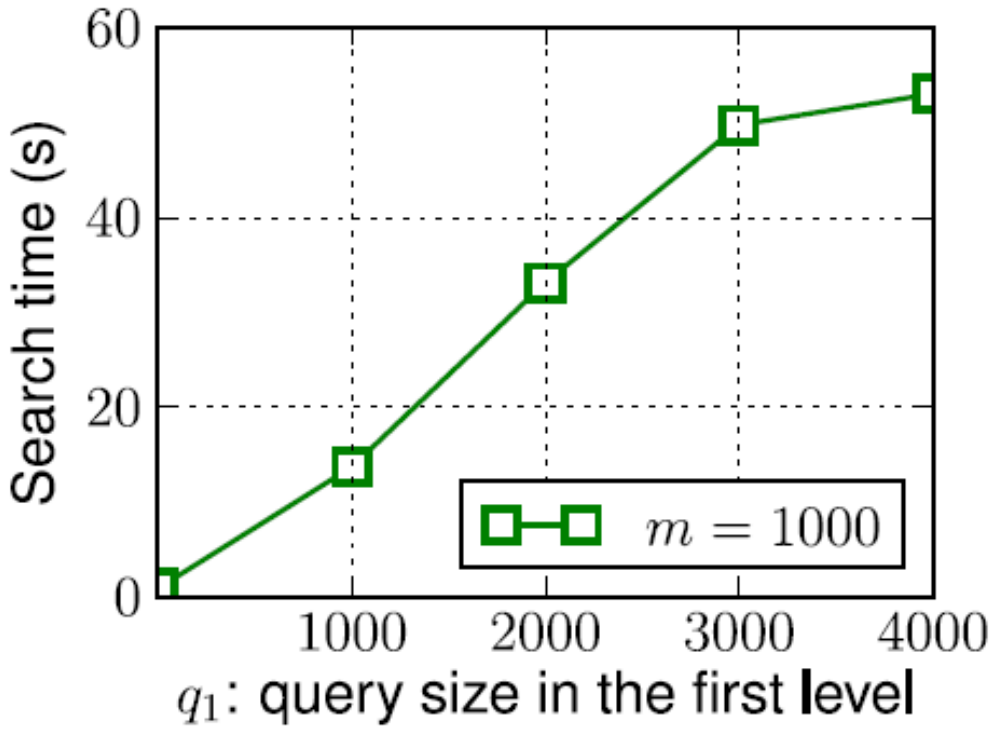
IV. Evaluation

Main parameters:

- Vector length m
- First-level query size q_1

Impact of m on Average Search Time (s)

$\|Q\| = m \times q_1$	m	Time
1×10^6	1,000	13.67
	100	1.50
	10	0.25



IV. Evaluation

Comparison among schemes

	Search Time (s)	Complexity	Token Size	Update
GR [8]	1,753	linear	0.96 KB	No
WLW [11]	1,583	logarithmic	20 KB	No
FastGeo	13.67	sublinear	132 KB	Yes

V. Conclusion

Major contributions of this paper:

1. FastGeo: a geometric range query scheme for encrypted spatial data is designed.

2. FastGeo supports not only efficient query for encrypted spatial data, but also update.

3. FastGeo is at least 100 times faster than previous schemes.