Методы обеспечения конфиденциальности пространственных данных в облаке у недоверенного провайдера, предоставляющие возможность выполнения пространственных запросов к этим данным

Андрей Матерухин, к.т.н.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет геодезии и картографии» (МИИГАиК)

Пространственные данные

- Модели пространства
  - Геодезические модели пространства
  - Евклидовы модели пространства

Методы индексации пространственных данных

Кластеризация объектов

- *R, R+ и R* - деревья*
- *Задание отношения линейного порядка (например, с помощью кривой Гильберта) и использование B, B+ и B* деревьев*

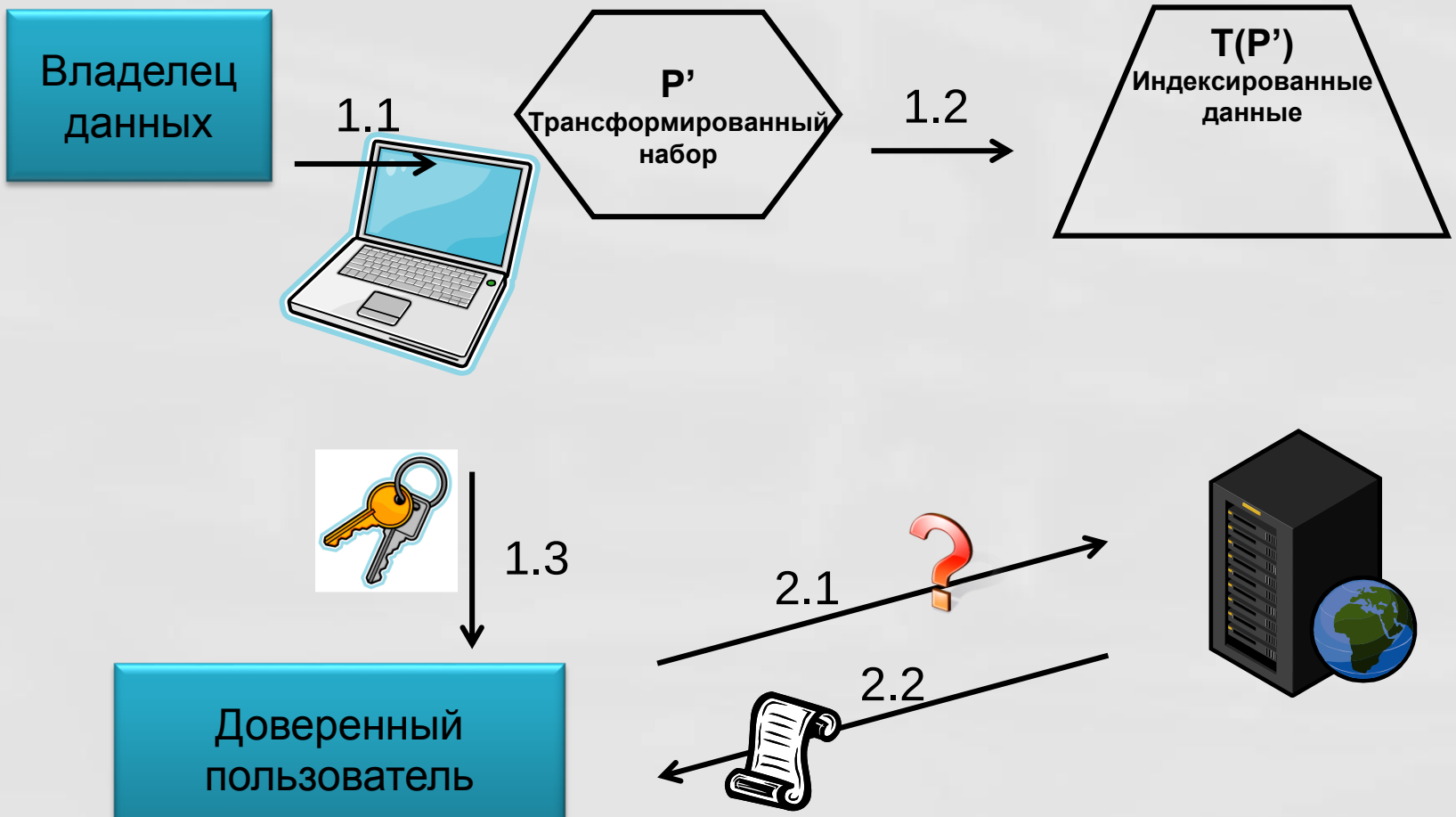
Декомпозиция пространства

- *kD - деревья*

Схемы, связанные с преобразованием пространства, излагаются на основе:

M. L. Yiu, G. Ghinita, C. S. Jensen and P. Kalnis, “Outsourcing Search Services on Private Spatial Data”, Proceeding of the 25th IEEE International Conference on Data Engineering, (2009) March 29-April 2, Shanghai, China.

Рассматриваемая схема взаимодействия



Решаемые задачи

- **Сделать возможным эффективное и точное выполнение запросов типа «выдать все объекты из набора P, находящиеся внутри диапазона $W = [x_l, x_h] \times [y_l, y_h]$»**
- **Сделать трудным восстановление исходного набора из трансформированного набора без знания ключа**

Модели атаки

Атакующий знает :

- Трансформированный набор P'

- Некоторое подмножество $S \subset P$

и соответствующее ему подмножество $S' \subset P'$

- S не совпадает с P и атакующий не может выбирать S

- **Tailored attack (специализированная атака)**

- Цель – определить точное исходное положение каждого объекта

- ***Предполагает, что атакующий знает метод трансформации***
- ***- Сводится к составлению системы уравнений***

- **General attack (общая атака)**
- ***Цель – определить приближенное исходное положение объектов в P'–S', основываясь на знании S и S'***
- ***Не предполагает каких-либо знаний о методе трансформации***

Общая атака (general attack)

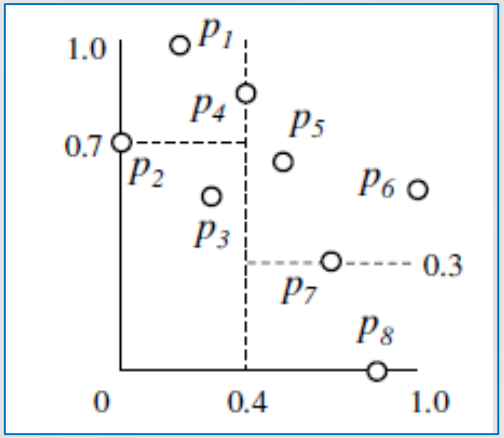
- Вектор (feature vector) V(p′, S′) для p′ ∈ P′ –S′
- V(p′, S′) = (dist(p′, s'_1), dist(p′, s'_2), ..., dist(p′, s'_m))
- Соответственно, для c из оригинального пространства
- V(c, S) = (dist(c, s_1), dist(c, s_2), ..., dist(c, s_m))
- Расхождение между c и p′ определяется как

$$\Phi(c, p') = L_1 \left(\frac{V(p', S')}{|V(p', S')|}, \frac{V(c, S)}{|V(c, S)|} \right)$$

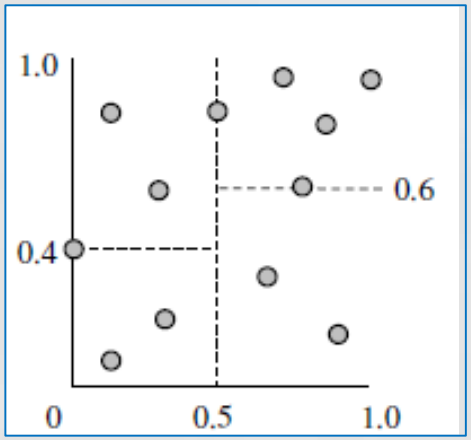
- где L_1 – это манхэттенское расстояние.
- Атакующий находит p* - прообразы точек p′ ∈ P′ в оригинальном пространстве, которые имеют min Φ(c, p′), а поскольку это, возможно, неоднозначно определяет местоположение, то дополнительно используется метод Монте-Карло.
- Ошибка атакующего оценивается, используя расстояние dist(p, p*).

Преобразование данных, основанное на иерархическом разбиении пространства

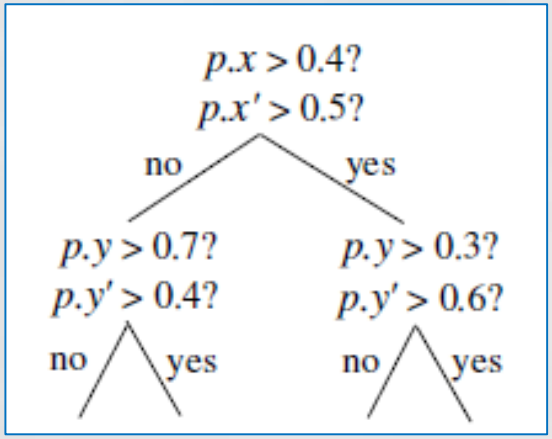
Исходный



Целевой

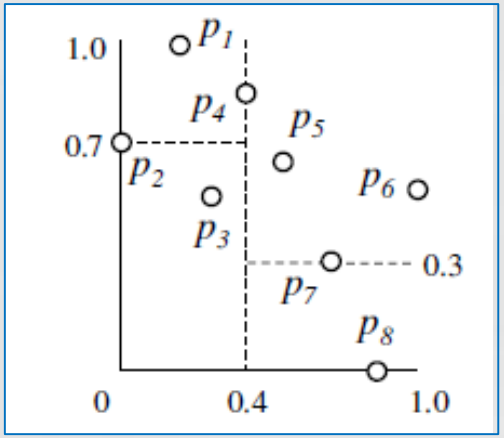


Дерево трансформации

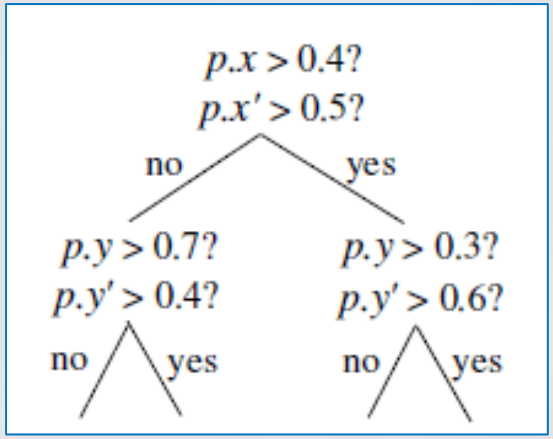


Преобразование данных, основанное на иерархическом разбиении пространства

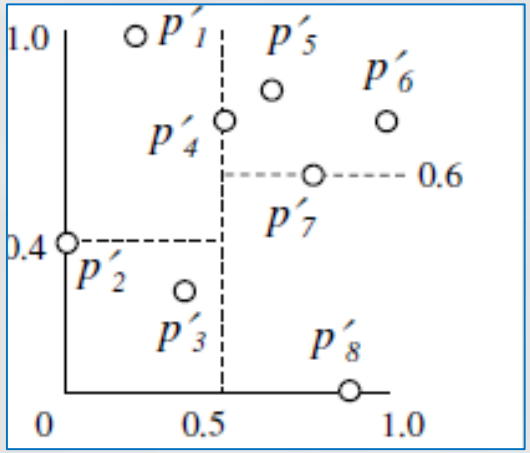
Исходный



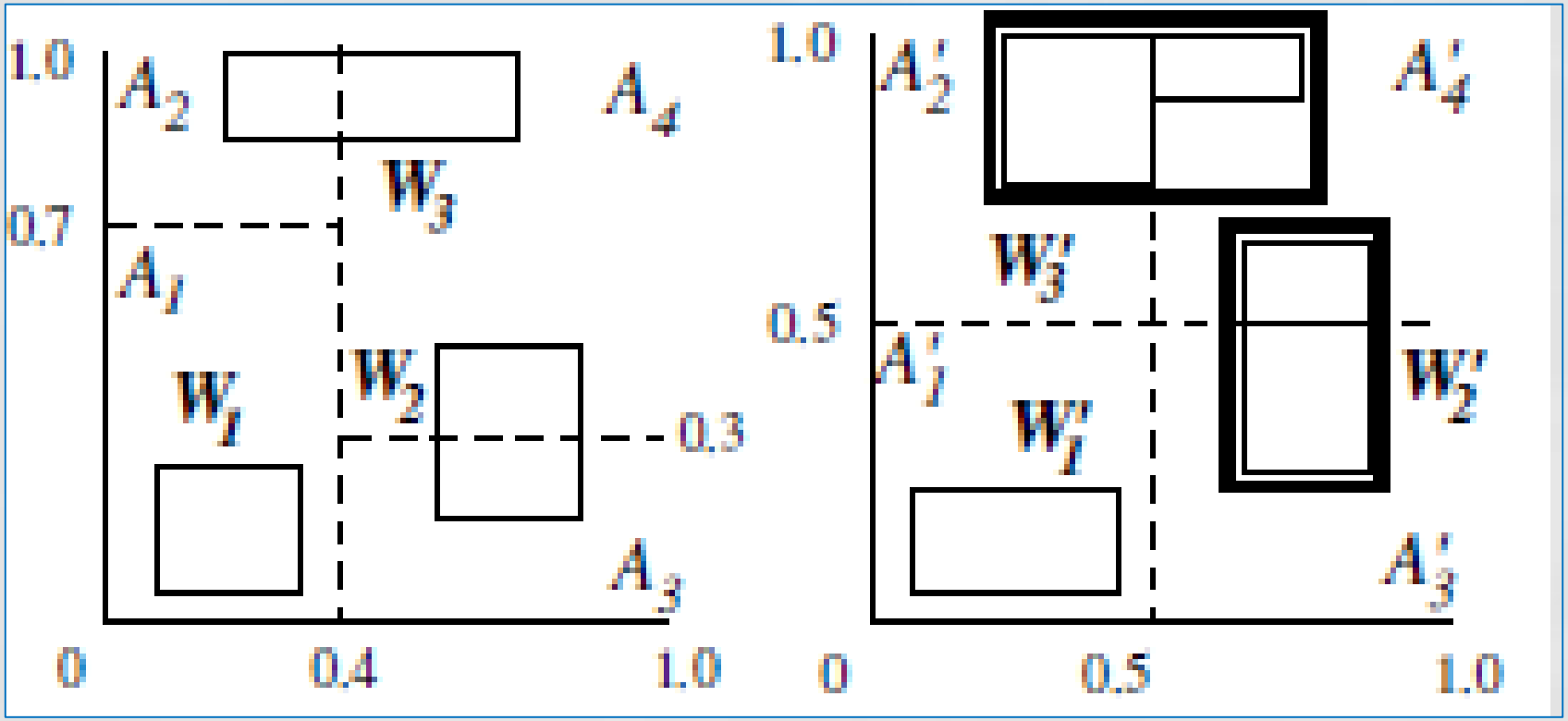
Дерево трансформации



Трансформированный

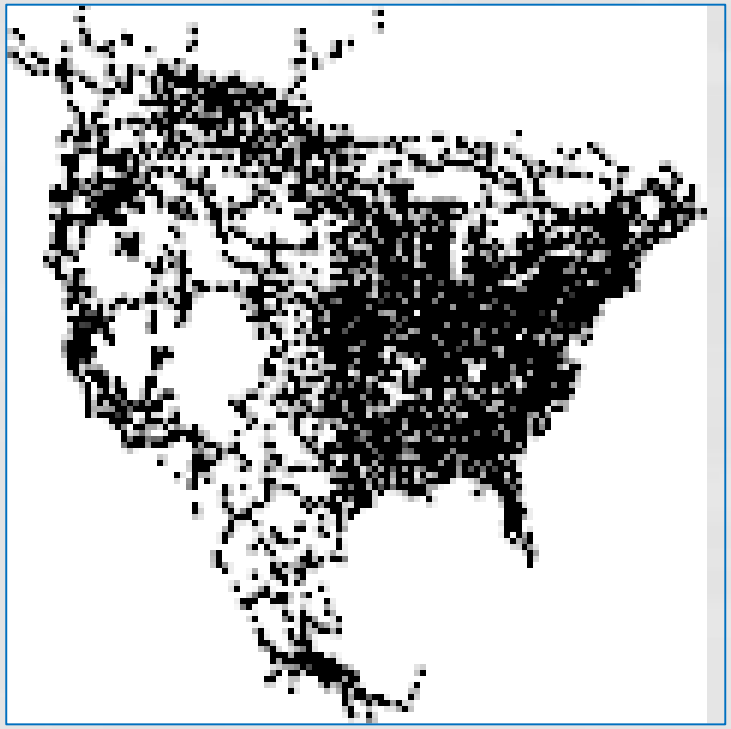


Трансформация запросов

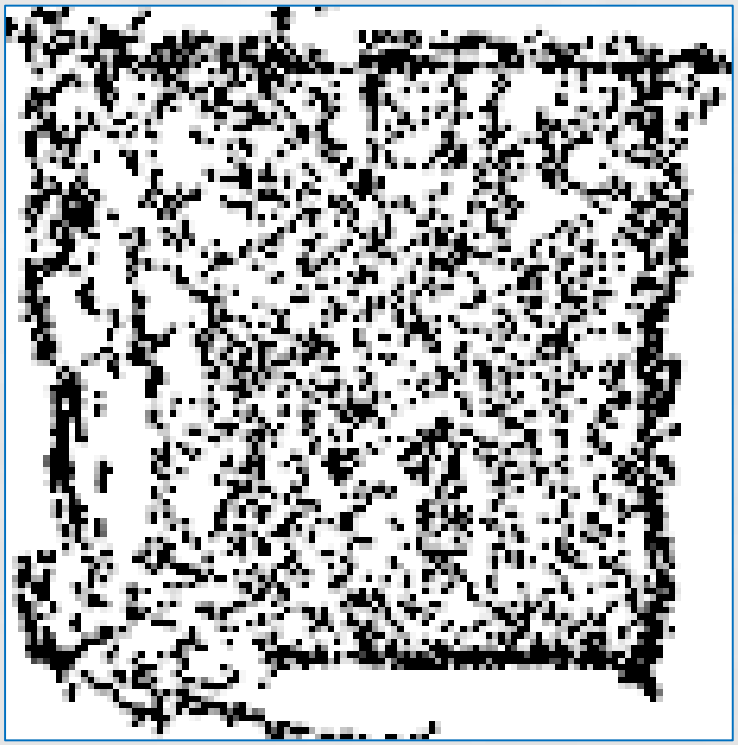


Пример преобразования данных, основанного на иерархическом разбиении пространства

Исходный



Преобразованный



Использовании криптографических хэш-функций для трансформации пространства (error-based transformation)

- Ключ – (ε, K_x, K_y), $\varepsilon \in [0, 1)$
- $p = (id, x, y)$
- $P' = (id, x', y')$
- $x' = (1 - \varepsilon) \cdot x + \varepsilon \cdot H(K_X \circ id)$
- $y' = (1 - \varepsilon) \cdot x + \varepsilon \cdot H(K_X \circ id)$

- Трансформация запросов

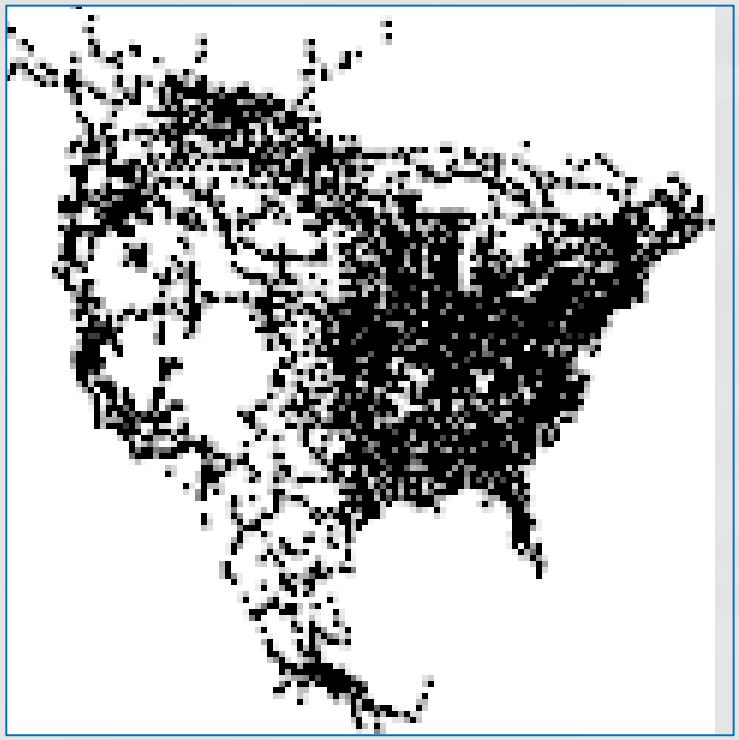
$W = [x_l, x_h] \times [y_l, y_h]$

$x'_l = (1 - \varepsilon) \cdot x_l \qquad x'_h = (1 - \varepsilon) \cdot x_h + \varepsilon$

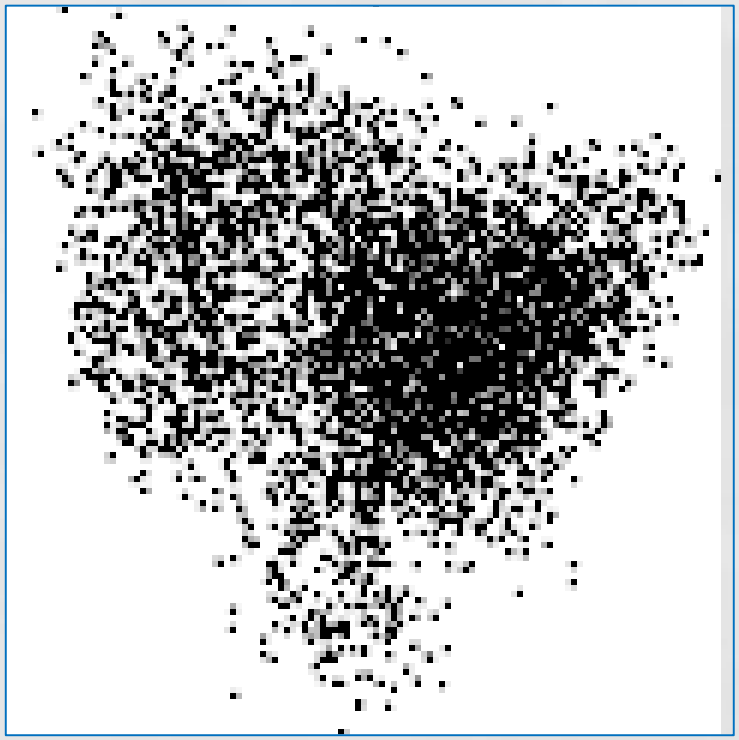
$y'_l = (1 - \varepsilon) \cdot y_l \qquad y'_h = (1 - \varepsilon) \cdot y_h + \varepsilon$

Пример ERB преобразования данных

Исходный



Преобразованный



Криптографические трансформации

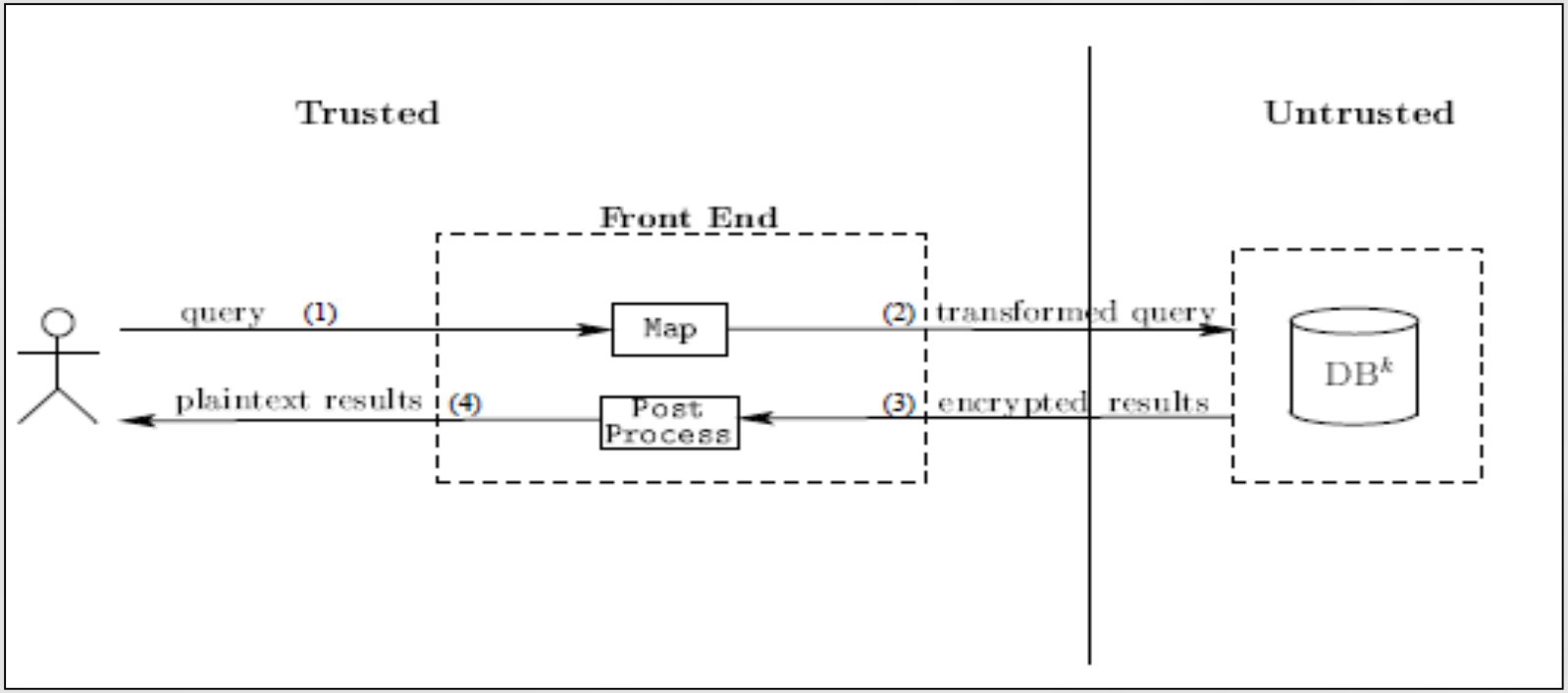
- E. Damiani, S. D. C. Vimercati, S. Jajodia, S. Paraboschi, P. Samarati. Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs. In CCS, 2003.

- A. Khoshgozaran and C. Shahabi. Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy. In SSTD, 2007.

- M. L. Yiu, G. Ghinita, C. S. Jensen and P. Kalnis, “Outsourcing Search Services on Private Spatial Data”, Proceeding of the 25th IEEE International Conference on Data Engineering, (2009) March 29-April 2, Shanghai, China.

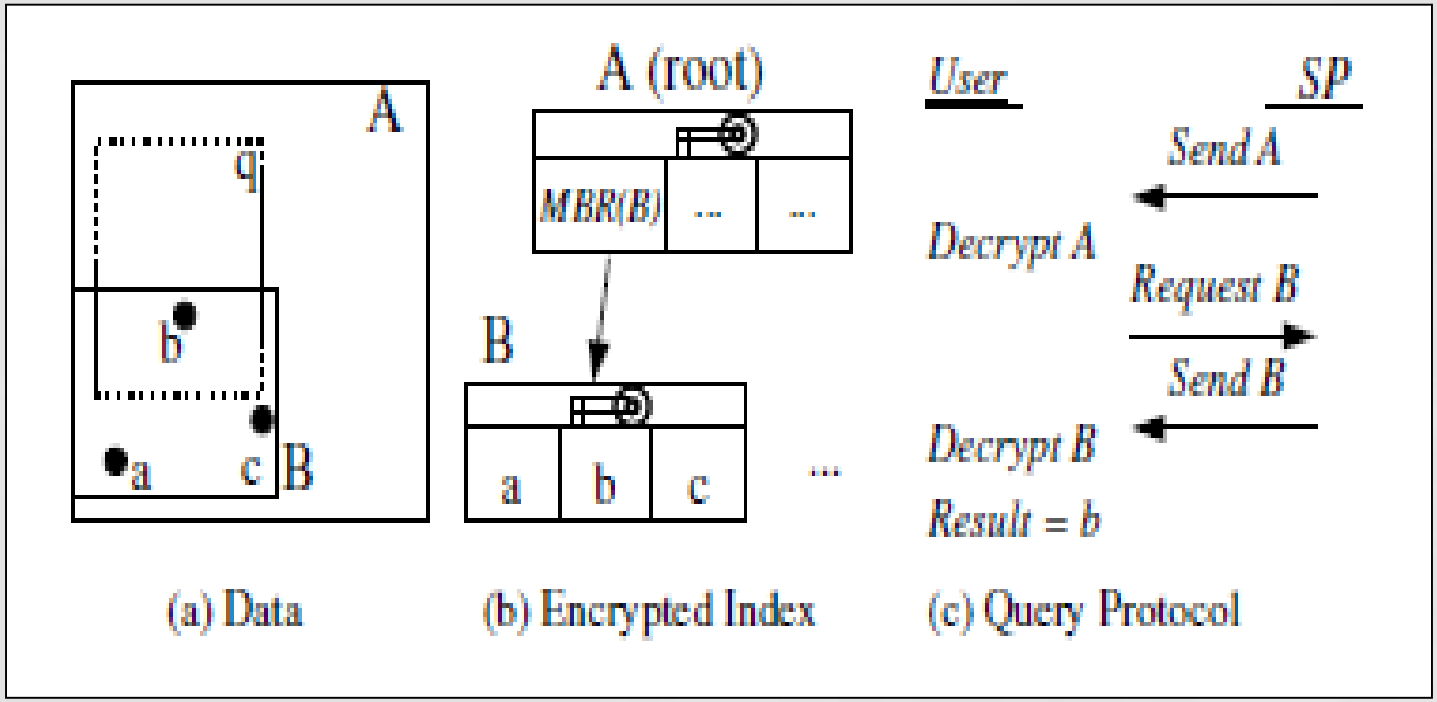
Криптографические трансформации

- Из E. Damiani, S. D. C. Vimercati, S. Jajodia, S. Paraboschi, P. Samarati. Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs. In CCS, 2003



Криптографические трансформации

- Из M. L. Yiu, G. Ghinita, C. S. Jensen and P. Kalnis, “Outsourcing Search Services on Private Spatial Data”, Proceeding of the 25th IEEE International Conference on Data Engineering, (2009) March 29-April 2, Shanghai, China.



Схема, основанная на идеях предикативного шифрования

- Boyang Wang; Ming Li; Haitao Wang; Hui Li "Circular Range Search on Encrypted Spatial Data", Distributed Computing Systems (ICDCS), 2015 IEEE 35th International Conference , pages: 794 – 795

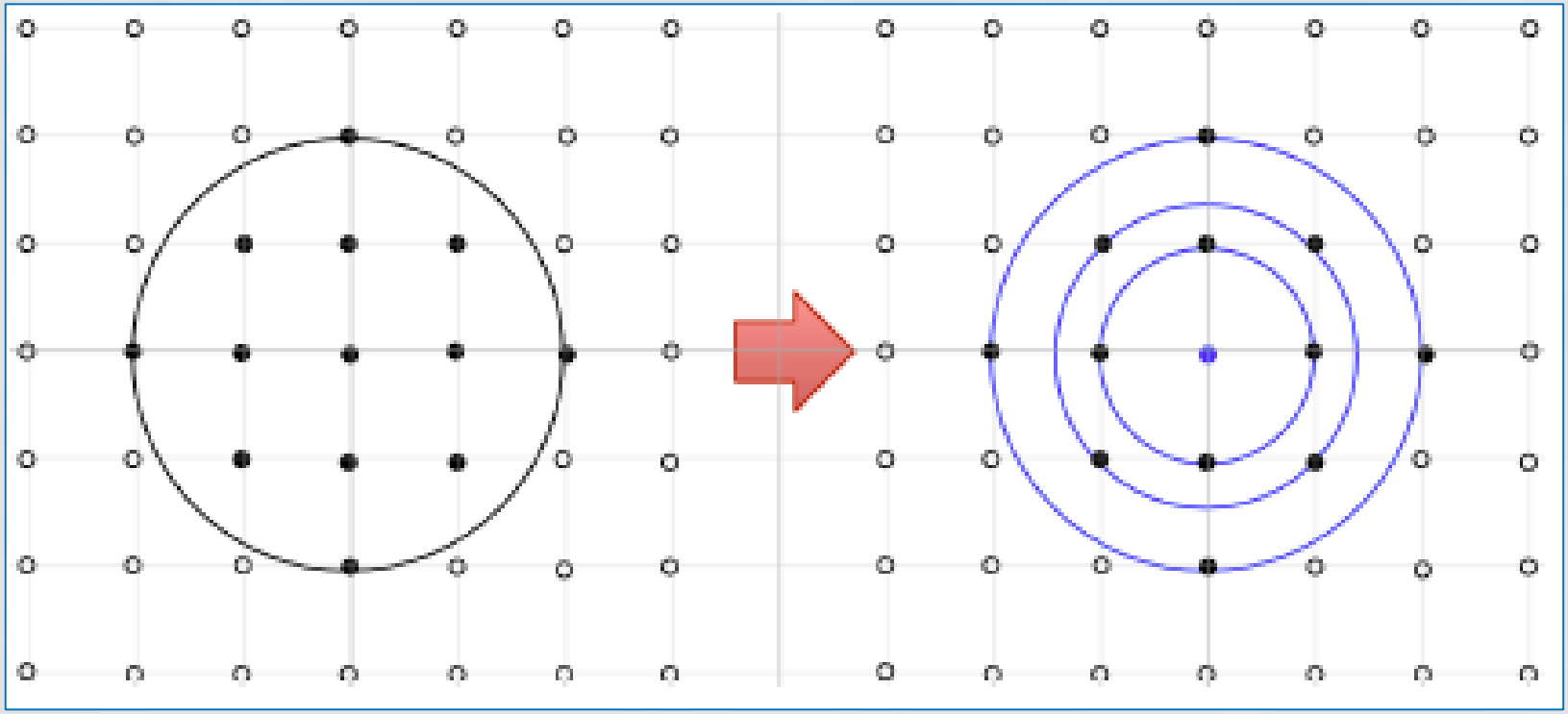
Использует результаты

- Emily Shen, Elaine Shi, and Brent Waters. 2009. Predicate Privacy in Encryption Systems. In Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography (TCC '09), Omer Reingold (Ed.). Springer-Verlag, Berlin, Heidelberg, 457-473. DOI=http://dx.doi.org/10.1007/978-3-642-00457-5_27

Краткое изложение

- **Основная идея предикативного шифрования : можно проверить f(u) = 1 или f(u) = 0, используя только шифротекст C(u).**
- **Shen, Shi и Waters разработали схему шифрования с общим ключом, которая основана на скалярном умножении векторов, связанных с текстом и с запросом.**
- **Li, Wang, Li на основе SSW предлагают свою схему шифрования Circle Predicate Encryption, которая позволяет проверить находится ли точка на границе круга, раскрывая только радиус этого круга и ничего больше.**

Основная идея использования Circle Predicate Encryption.



Спасибо за внимание !!!