Abstract

Database query evaluation over encrypted data has received a lot of attention recently. Order-Preserving Encryption (OPE) and Order-Revealing Encryption (ORE) are two important encryption schemes that have been proposed in these areas. This paper can provide very efficient query execution, but at the same time may lack new information to users. Many researchers have been interested in them and developed many algorithms and protocols to make them more useful. The former are based on a fully homomorphic encryption (FHE) scheme and the latter are based on non-interactive zero-knowledge (NIZK) proofs. We focus on the former and give an overview of their state of the art together with a comparison among several important examples. We analyze and compare them both theoretically and experimentally and measure their performance via database indexing and query evaluation. We report not only execution time but also I/O performance, communication amount, and usage of cryptographic primitive operations. The comparison results interesting people concerning the relative security and performance of these approaches in database settings.

OPE: Order-Preserving Encryption

An Order-Preserving Encryption (OPE) scheme is a tuple of polynomial-time algorithms $(\text{Encrypt}, \text{Decrypt})$. Here $x \rightarrow y$ means that $x$ encrypts to $y$ and $y$ decrypts to $x$.

- $\text{Encrypt}(x)$: takes a message $x$ and outputs an encryption $\text{Encrypt}(x)$.
- $\text{Decrypt}(y)$: takes a ciphertext $y$ and outputs the original message $x = \text{Decrypt}(y)$.

A well-known example is the identity function $x \rightarrow x$.

ORE: Order-Revealing Encryption

An Order-Revealing Encryption (ORE) scheme is defined by a tuple of polynomial-time algorithms $(\text{Encrypt}, \text{Decrypt})$. Here $x \rightarrow y$ means that $x$ encrypts to $y$ and $y$ decrypts to $x$.

- $\text{Encrypt}(x)$: takes a message $x$ and outputs a ciphertext $\text{Encrypt}(x)$.
- $\text{Decrypt}(y)$: takes a ciphertext $y$ and outputs the original message $x = \text{Decrypt}(y)$.

ORE schemes are classified into two types:

- Deterministic or non-interactive ORE
- Probabilistic or interactive ORE

Deterministic ORE

- $\text{Encrypt}(x) \rightarrow \text{Encrypt}(x)$
- $\text{Decrypt}(y) \rightarrow y$

Probabilistic ORE

- $\text{Encrypt}(x) \rightarrow \text{Encrypt}(x')$
- $\text{Decrypt}(y) \rightarrow y'$

ORE schemes are classified into two types:

- Deterministic or non-interactive ORE
- Probabilistic or interactive ORE

Deterministic ORE

- $\text{Encrypt}(x) \rightarrow \text{Encrypt}(x)$
- $\text{Decrypt}(y) \rightarrow y$

Probabilistic ORE

- $\text{Encrypt}(x) \rightarrow \text{Encrypt}(x')$
- $\text{Decrypt}(y) \rightarrow y'$

ORE schemes are classified into two types:

- Deterministic or non-interactive ORE
- Probabilistic or interactive ORE

Deterministic ORE

- $\text{Encrypt}(x) \rightarrow \text{Encrypt}(x)$
- $\text{Decrypt}(y) \rightarrow y$

Probabilistic ORE

- $\text{Encrypt}(x) \rightarrow \text{Encrypt}(x')$
- $\text{Decrypt}(y) \rightarrow y'$

ORE schemes are classified into two types:

- Deterministic or non-interactive ORE
- Probabilistic or interactive ORE

Deterministic ORE

- $\text{Encrypt}(x) \rightarrow \text{Encrypt}(x)$
- $\text{Decrypt}(y) \rightarrow y$

Probabilistic ORE

- $\text{Encrypt}(x) \rightarrow \text{Encrypt}(x')$
- $\text{Decrypt}(y) \rightarrow y'$