Information Sciences 387 (2017) 266–279

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Semi-order preserving encryption

Ce Yang, Weiming Zhang*, Nenghai Yu

CAS Key Laboratory of Electro-magnetic Space Information, University of Science and Technology of China, Hefei, 230026, China

ARTICLE INFO

Article history:
Received 31 December 2015
Revised 11 October 2016
Accepted 14 December 2016
Available online 15 December 2016

Keywords:
Order preserving encryption
Semi-order preserving encryption

ABSTRACT

Order preserving encryption (OPE) is a kind of encryption designed to support searches on ciphertexts. OPE encrypts plaintexts to ciphertexts with the same order, making it possible to efficiently compare ciphertexts without decryption. Because of its efficiency, OPE has been used in systems aimed at practical use. However, even though many OPE schemes have been proposed, all suffer from security and ciphertext expansion problems.

This paper proposes the notation of semi-order preserving encryption (SOPE) as a substitute for OPE. SOPE uses a semi-order preserving condition instead of strict order preserving condition to support a range query on ciphertexts. By this means, SOPE can enhance security and reduce storage cost with some sacrifice of precision. The loss of precision can be eliminated with the cost of extra communication and computation, because it is easy to generate a query on ciphertexts including all required plaintexts.

To study the relationship among precision, security and ciphertext expansion, we introduce semi-order preserving degree d, which measures the difference between SOPE and OPE. The theoretical derivation shows that security will increase with d, while precision and ciphertext expansion will decrease with d. Thus SOPE can balance precision, security and ciphertext expansion by adjusting semi-order preserving degree d according to a concrete condition. Finally, we present an implementation of SOPE.

1. Introduction

Encryption is among the most common technologies used to protect the privacy of data stored on untrusted servers, such as in cloud computing [2]. While protecting data privacy, encryption makes data processing, such as searching difficult. To solve this problem, computing on encrypted data, such as homomorphic encryption [9], is proposed. Fully homomorphic encryption supports adding and multiplying ciphertexts; nevertheless, it suffers from bad performance. A more practical solution is to support only a specific subset of operations on ciphertext. Searching is among the most common operations in data processing, thus searchable encryption [5,10,18], the cryptographic primitive supporting searching on encrypted data, has attracted the interests of many researchers.

Order preserving encryption (OPE) scheme is a searchable encryption applied on numeric data. OPE preserves the order relationship of plaintexts to support comparison of the ciphertexts. In this way, computation based on comparison, such as range queries, and skyline queries [6] can be executed on the OPE ciphertext. Using OPE, range queries on plaintexts can be substituted by range queries on ciphertexts, and search can be accelerated to the logarithmic level by indexing

* Corresponding author.
E-mail addresses: yangce@mail.ustc.edu.cn (C. Yang), zhangwm@mail.ustc.edu.cn, zhangwm@ustc.edu.cn (W. Zhang), ynh@ustc.edu.cn (N. Yu).

http://dx.doi.org/10.1016/j.ins.2016.12.025
0020-0255/

on ciphertexts or binary search. Because of its efficiency, OPE has been adopted in CryptDB system [16] developed by the Massachusetts Institute of Technology (MIT), Encrypted BigQuery [11] developed by Google, and many other systems aimed at practical use [8,23,24].

The concept of OPE was first proposed by Agrawal et al. [1] as a solution to range query on an encrypted database. Boldyreva et al. [3,4] discussed the security of OPE in provable-security means. They proposed a scheme, which is a pseudorandom order-preserving function secure against chosen-ciphertext attack, and they implemented it by lazy-sampling a hypergeometric distribution. Popa et al. [17] proposed an ideal secure construction of OPE. Their scheme is indistinguishable under ordered chosen-plaintext attack, such that the adversary cannot distinguish between 2 ciphertext sequences encrypted from the plaintext sequences of the same order. Above-mentioned OPE schemes are all deterministic encryption schemes, or one-to-one OPE. Wang et al. [20] proposed a one-to-many scheme and applied it to the reverse index of text retrieval.

Despite the excellent search speed, OPE still suffers from security problems and ciphertext expansion. To guarantee security, OPE maps the plaintext space to a far larger ciphertext space, leading to vast storage cost caused by ciphertext expansion. On the other hand, OPE is still vulnerable to inference attack, which combines additional background knowledge such as language statistics with ciphertext to recover plaintext, even though the ciphertext space is large enough. Naveed et al. [15] evaluated a series of attacks empirically in an electronic medical records scenario using real patient data encrypted by one-to-one OPE. Li et al. [13] used a differential attack to recover the plaintext of an encrypted index generated by a one-to-many OPE.

Various constructions [12,14,21] have been proposed to address these problems. However, improvement of all these OPE constructions is limited by the strictly order-preserving condition. In this paper, we propose the concept of semi-order preserving encryption (SOPE) as a substitute of OPE. SOPE is a new cryptographic primitive similar to OPE; however, SOPE uses a semi-order preserving condition, instead of an order-preserving condition, to enable query search on ciphertexts. Semi-order preserving is weaker than order preserving, and SOPE can get better security or smaller ciphertext expansion than OPE can with some communication and local computation costs.

Our contribution includes the following:

1. We propose a new cryptographic primitive SOPE, which is a generalization of OPE. We demonstrate some basic property of SOPE that also applies to OPE.
2. We define a parameter, semi-order preserving degree d, to measure the difference between SOPE and OPE. We then study the relationship between semi-order preserving degree and the security, precision, ciphertext expansion of SOPE.
3. Finally, we propose a construction of SOPE. The construction works like stream encryption. An encryption key is chosen at the beginning of the encryption, and a decryption key is generated after the encryption. With the decryption key, the plaintexts can be fully recovered. The experiments show that the security, precision, and ciphertext expansion can be adjusted by modifying semi-order preserving degree d.

The rest of this paper is organized as follows: Section 2 gives the definition and basic property of SOPE. Section 3 gives the measurement of SOPE and studies the relationship among different parameters. In Section 4, we propose a construction of SOPE. Sections 5 concludes this paper.

2. Semi-order preserving encryption

2.1. Definition

An OPE scheme is a mapping from plaintext space $\mathbb{X}$ to ciphertext space $\mathbb{Y}$. Each plaintext $x \in \mathbb{X}$ is mapped to a random-sized nonoverlapping interval bucket in $\mathbb{Y}$, then a ciphertext c is chosen within the bucket. In this paper, we focus on OPE and SOPE on integers. For convenience, we use interval $[a, b]$ to represent integers in the interval, i.e. $\{a, a+1, \ldots, b\}$, when we talk about plaintext and ciphertext. For example, we say plaintext $x \in [1, 3]$ if $x \in \{1, 2, 3\}$. Similarly, $\|\mathbb{S}\|$ denotes the number of integers in set $\mathbb{S}$. As in most works of OPE, we assume the plaintext space satisfies $\mathbb{X} = [1, N]$ and the ciphertext space satisfies $\mathbb{Y} = [1, M]$, i.e., they are both intervals on integers beginning from 1. N and M are the sizes of plaintext and ciphertext space, respectively.

A deterministic OPE scheme always assigns the same ciphertext y in the bucket for the same plaintext x, while a probabilistic or one-to-many OPE scheme chooses a random value within the ciphertext bucket each time.

We can use the probability distribution to describe a probabilistic encryption. Denote the plaintext and ciphertext probability density function as $P_X(x)$ and $P_Y(y)$, respectively, and the plaintext and ciphertext cumulative function as $P_{CX}(x)$ and $P_{CY}(y)$, respectively. For convenience, we assume $P_{CX}(0) = P_{CY}(0) = 0$, such that $P_X(1) = P_{CX}(1) - P_{CX}(0)$ and $P_Y(1) = P_{CY}(1) - P_{CY}(0)$. The property of OPE is determined by the conditional probability function $P_{Y|X}(x, y)$ or joint probability $P_{X,Y}(x, y)$ when P_X is given. For convenience, we use $P(x|y)$ and $P(y|x)$ to represent $P_{X|Y}(x, y)$ and $P_{Y|X}(x, y)$, respectively.

Using these notations, the order preserving feature can be described as follows: if f: $x \to y$ is an OPE, $x_1 < x_2$, $y_1 \geq y_2$, and $P_{X,Y}(x_1, y_1) > 0$, then $P_{X,Y}(x_2, y_2) = 0$.

If we loosen up this constraint, we can get the semi-order preserving feature. For a SOPE f: $x \to y$ and every $x_1 < x_2$, $y_1 > y_2$, if $P_{X,Y}(x_1, y_1) > 0$, then $P_{X,Y}(x_2, y_2) = 0$.

The difference between SOPE and OPE is that SOPE may encrypt 2 different plaintexts $x_1 \neq x_2$ to the same ciphertext value y, whereas this will never happen on OPE.

2.2. Basic property

Here we discuss the basic property of SOPE.

We analyze how plaintext and ciphertext distribution affect the encryption, i.e., the relationship between $P_X(x)$, $P_Y(y)$, and $P_{X,Y}(x, y)$. For a SOPE, the joint probability distribution $P_{X,Y}(x, y)$ can be derived from the plaintext distribution $P_X(x)$ and ciphertext distribution $P_Y(y)$.

To prove this conclusion, we start from a lemma.

Lemma 1. *For a SOPE f: $X \to Y$, $x_1, x_2, x_3, x_4 \in \mathbb{X}$, $y_1, y_2, y_3, y_4 \in \mathbb{Y}$, if $x_2 < x_3$ and $y_2 < y_3$, then*

$$\sum_{i=x_1}^{x_2} \sum_{j=y_3}^{y_4} P_{X,Y}(i, j) = 0, \tag{1}$$

or

$$\sum_{i=x_3}^{x_4} \sum_{j=y_1}^{y_2} P_{X,Y}(i, j) = 0. \tag{2}$$

Proof. When

$$\sum_{i=x_1}^{x_2} \sum_{j=y_3}^{y_4} P_{X,Y}(i, j) = 0, \tag{3}$$

the lemma is proved.

When

$$\sum_{i=x_1}^{x_2} \sum_{j=y_3}^{y_4} P_{X,Y}(i, j) > 0, \tag{4}$$

there exists x_0, y_0, such that $x_0 \in [x_1, x_2]$, $y_0 \in [y_3, y_4]$ and

$$P_{X,Y}(x_0, y_0) > 0. \tag{5}$$

For $i \in [x_3, x_4]$ and $j \in [y_1, y_2]$, because

$$i \geq x_3 > x_2 \geq x_0 \tag{6}$$

and

$$j \leq y_2 < y_3 \leq y_0, \tag{7}$$

according to the SOPE condition, we have

$$P_{X,Y}(i, j) = 0. \tag{8}$$

Thus

$$\sum_{i=x_3}^{x_4} \sum_{j=y_1}^{y_2} P_{X,Y}(i, j) = 0, \tag{9}$$

and the lemma is proved. □

Lemma 1 means that, if the arrangement of two sub-matrices of the joint probability is anti-diagonal, then either of the two sub-matrices is zero matrix. With the help of Lemma 1, we can prove Lemma 2, which describes the relationship between the cumulative distribution of joint probability $P_{CX,CY}(x, y)$ and marginal distribution $P_{CX}(x)$, $P_{CY}(y)$.

Lemma 2. *For a SOPE f: $X \to Y$,*

$$P_{CX,CY}(x, y) = \min\{P_{CX}(x), P_{CY}(y)\}. \tag{10}$$

Proof. We have

$$\begin{aligned} P_{CX}(x) &= \sum_{i=0}^{x} P_X(i) \\ &= \sum_{i=0}^{x} \sum_{j=0}^{M} P_{X,Y}(i, j) \end{aligned}$$

Table 1
joint distribution.

	0	...	$y-1$	y	$y+1$	...	M
0							
...		R_{00}		R_{01}		R_{02}	
$x-1$							
x		R_{10}		R_{11}		...	
$x+1$							
...		R_{20}		...		...	
N							

$$= \sum_{i=0}^{x}\sum_{j=0}^{y} P_{X,Y}(i,j) + \sum_{i=0}^{x}\sum_{j=y+1}^{M} P_{X,Y}(i,j)$$

$$= P_{CX,CY}(x,y) + \sum_{i=0}^{x}\sum_{j=y+1}^{M} P_{X,Y}(i,j). \tag{11}$$

Similarly,

$$P_{CY}(y) = P_{CX,CY}(x,y) + \sum_{i=x+1}^{N}\sum_{j=0}^{y} P_{X,Y}(i,j). \tag{12}$$

Because $x < x+1$ and $y < y+1$, according to Lemma 1,

$$\sum_{i=0}^{x}\sum_{j=y+1}^{M} P_{X,Y}(i,j) = 0, \tag{13}$$

or

$$\sum_{i=x+1}^{N}\sum_{j=0}^{y} P_{X,Y}(i,j) = 0. \tag{14}$$

Thus,

$$P_{CX}(x) = P_{CX,CY}(x,y), \tag{15}$$

or

$$P_{CY}(y) = P_{CX,CY}(x,y), \tag{16}$$

i.e.,

$$P_{CX,CY}(x,y) = \min\{P_{CX}(x), P_{CY}(y)\}. \tag{17}$$

Thus the lemma is proved. □

Lemma 2 indicates that $P_{CX,\,CY}(x,\,y)$ is determined by $P_{CX}(x)$ and $P_{CY}(y)$. Knowing cumulative distribution $P_{CX,\,CY}(x,\,y)$, the joint probability distribution $P_{X,\,Y}(x,\,y)$ can be determined by

$$P_{X,Y}(x,y) = P_{CX,CY}(x,y) + P_{CX,CY}(x-1,y-1) - P_{CX,CY}(x-1,y) - P_{CX,CY}(x,y-1). \tag{18}$$

However, there is a simpler result.

Theorem 1. *For a SOPE f: $X \to Y$, if $P_{X,\,Y}(x,\,y) > 0$, then*

$$P_{X,Y}(x,y) = \min\{P_{CX}(x), P_{CY}(y)\} - \max\{P_{CX}(x-1), P_{CY}(y-1)\}. \tag{19}$$

If $P_{X,Y}(x,y) = 0$, then

$$\min\{P_{CX}(x), P_{CY}(y)\} - \max\{P_{CX}(x-1), P_{CY}(y-1)\} \le 0. \tag{20}$$

Proof. We can divide the joint probability distribution to nine different parts as Table 1.

The sum of each part is

$$R_{00} = P_{CX,CY}(x-1,y-1),$$

$$R_{01} = \sum_{i=0}^{x-1} P_{X,Y}(i,y),$$

$$
\begin{aligned}
R_{10} &= \sum_{j=0}^{y-1} P_{X,Y}(x, j),\\
R_{11} &= P_{X,Y}(x, y),\\
R_{02} &= \sum_{i=0}^{x-1} \sum_{j=y+1}^{M} P_{X,Y}(i, j),\\
R_{20} &= \sum_{i=x+1}^{N} \sum_{j=0}^{y-1} P_{X,Y}(i, j).
\end{aligned} \tag{21}
$$

We can represent $P_{CX,\,CY}$, P_{CX} and P_{CY} using Eq. (21). We have

$$
\begin{aligned}
P_{CX,CY}(x, y) &= R_{00} + R_{01} + R_{10} + R_{11},\\
P_{CX}(x-1) &= R_{00} + R_{01} + R_{02},\\
P_{CY}(y-1) &= R_{00} + R_{10} + R_{20}.
\end{aligned} \tag{22}
$$

Because $x - 1 < x + 1$ and $y + 1 > y - 1$, according to Lemma 1, $R_{01} = 0$ or $R_{10} = 0$. We assume

$$R_{01} = 0 \tag{23}$$

here, and similar conduction can be made if $R_{10} = 0$.

When $P_{X,\,Y}(x, y) > 0$, because $x - 1 < x$ and $y + 1 > y$, according to Lemma 1,

$$R_{02} = 0. \tag{24}$$

Similarly,

$$R_{20} = 0. \tag{25}$$

Combining Eqs. (22), (23), and (24),

$$
\begin{aligned}
P_{CX}(x-1) &= R_{00} + R_{01} + R_{02}\\
&= R_{00}.
\end{aligned} \tag{26}
$$

Combining Eqs. (22) and (25),

$$
\begin{aligned}
P_{CY}(y-1) &= R_{00} + R_{10} + R_{20}\\
&= R_{00} + R_{10}.
\end{aligned} \tag{27}
$$

Thus,

$$\max\{P_{CX}(x-1), P_{CY}(y-1)\} = R_{00} + R_{10}, \tag{28}$$

and

$$
\begin{aligned}
P_{X,Y}(x, y) &= R_{11}\\
&= (R_{00} + R_{01} + R_{10} + R_{11}) - (R_{00} + R_{01} + R_{10})\\
&= P_{CX,CY}(x, y) - (R_{00} + R_{10})\\
&= \min\{P_{CX}(x), P_{CY}(y)\} - \max\{P_{CX}(x-1), P_{CY}(y-1)\}.
\end{aligned} \tag{29}
$$

When $P_{X,Y}(x, y) = 0$,

$$
\begin{aligned}
P_{CY}(y-1) &= R_{00} + R_{10} + R_{20}\\
&\geq R_{00} + R_{10}\\
&= R_{00} + R_{10} + R_{01} + R_{11}\\
&= \min\{P_{CX}(x), P_{CY}(y)\}.
\end{aligned} \tag{30}
$$

Thus,

$$
\begin{aligned}
\min\{P_{CX}(x), P_{CY}(y)\} &\leq P_{CX}(x-1)\\
&\leq \max\{P_{CX}(x-1), P_{CY}(y-1)\}.
\end{aligned} \tag{31}
$$

If $R_{10} = 0$, after similar conduction, we will have the same conclusion.

In summary, Theorem 1 is proved. □

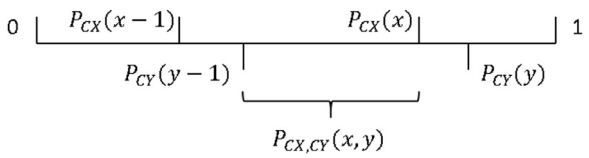

Fig. 1. An example of $P_{CX,\,CY}(x,\,y)$.

Corollary 1.

$$P_{X,Y}(x,y) = \|[P_{CX}(x-1), P_{CX}(x)] \cap [P_{CY}(y-1), P_{CY}(y)]\|. \tag{32}$$

Proof. When $P_{X,\,Y}(x,\,y) > 0$, the right-hand side of Eq. (32) equals the right-hand side of Eq. (19). When $P_{X,Y}(x,y) = 0$, the right-hand side of Eq. (32) equals 0. Thus Eq. (32) is equivalent to Theorem 1. □

We show an example in Fig. 1. The joint probability distribution $P_{X,\,Y}(x,\,y)$ can be calculated from the marginal distribution $P_X(x)$ and $P_Y(y)$ using Theorem 1 in linear time.

3. Property of SOPE

In this section, we define precision and security metrics for a SOPE, and study the relationship between precision, security, and ciphertext expansion of SOPE. To do so, first we introduce semi-order preserving degree d, which measures the difference between OPE and SOPE, and then analyze the relationship between the semi-order preserving degree and abovementioned quantities. The theoretical results show that we can get the trade-off between the precision, security, and ciphertext expansion by adjusting d.

For a SOPE f: $X \to Y$, denote the plaintext and ciphertext distribution with P_X and P_Y separately. Assume the plaintext space satisfies $\mathbb{X} = [1, N]$ and the ciphertext space satisfies $\mathbb{Y} = [1, M]$, then $N = \|\mathbb{X}\|$ and $M = \|\mathbb{Y}\|$. As mentioned, the property of SOPE is related to the ciphertext distribution. Here we assume the ciphertext follows a uniform distribution, i.e., $P_Y(y) = 1/M$.

3.1. Semi-order preserving degree

The ciphertext space of SOPE can be divided into 2 sets, the order preserving set $\mathbb{S}$ and the semi-order preserving set $\mathbb{D}$.

The order preserving set $\mathbb{S}$ is the set of ciphertexts on which the order preserving feature holds. If $x_1 \neq x_2$, $y \in \mathbb{S}$, and $P_{X,\,Y}(x_1,\,y) > 0$, then $P_{X,Y}(x_2, y) = 0$. The semi-order preserving set $\mathbb{D}$ consists of the other elements. If $y \in \mathbb{D}$, then $x_1 < x_2$ exists satisfying $P_{X,\,Y}(x_1,\,y) > 0$, $P_{X,\,Y}(x_2,\,y) > 0$.

A SOPE behaves just like OPE scheme on the order preserving set $\mathbb{S}$. The size of the semi-order preserving set can be used to measure the difference between OPE and SOPE.

The semi-order preserving degree d is defined as

$$d = \sum_{y \in \mathbb{D}} P_Y(y). \tag{33}$$

When $d = 0$, SOPE degenerates to OPE. When $d = 1$, all the possible ciphertexts correspond to 2 or more plaintexts.

As shown in Theorem 1, the property of SOPE is completely determined by the marginal distribution. This implies we can judge if a ciphertext is in the order preserving set from marginal distribution.

We have the following theorem:

Theorem 2. *If f: $X \to Y$ is a SOPE, $y \in \mathbb{Y}$, and there exists x such that*

$$P_{CX}(x-1) \le P_{CY}(y-1) \le P_{CY}(y) \le P_{CX}(x), \tag{34}$$

then y is in the order preserving set $\mathbb{S}$.

If there exists x such that

$$P_{CY}(y-1) < P_{CX}(x) < P_{CY}(y), \tag{35}$$

then y is in the semi-order preserving set $\mathbb{D}$.

Proof. The theorem describes 2 different cases.

1. There exists x, such that

$$P_{CX}(x-1) \le P_{CY}(y-1) \le P_{CY}(y) \le P_{CX}(x). \tag{36}$$

Then $P_{X,Y}(x, y) > 0$. For $i \le x-1$,

$$P_{CX}(i) \le P_{CX}(x-1) \le P_{CY}(y-1), \tag{37}$$

thus,

$$\begin{aligned}\min\{P_{CX}(i), P_{CY}(y)\} &\le \min\{P_{CY}(y-1), P_{CY}(y)\} \\ &= P_{CY}(y-1).\end{aligned} \tag{38}$$

We have

$$\max\{P_{CY}(y-1), P_{CX}(i-1)\} \ge P_{CY}(y-1). \tag{39}$$

Combining Theorem 1 with Eqs. (38) and (39), for $i \le x-1$,

$$P_{X,Y}(i, y) = 0. \tag{40}$$

Similarly, for $i \ge x+1$,

$$P_{X,Y}(i, y) = 0. \tag{41}$$

Combining Eqs. (40) and (41), we have

$$P(X = i|Y = y) = \begin{cases} 1 & i = x \\ 0 & i \ne x \end{cases} \tag{42}$$

i.e., y is in the order preserving set $\mathbb{S}$.

2. There exists x, such that

$$P_{CY}(y-1) < P_{CX}(x) < P_{CY}(y). \tag{43}$$

In such a situation,

$$P_{X,Y}(x, y) > 0, \tag{44}$$

and

$$P_{X,Y}(x+1, y) > 0. \tag{45}$$

Thus $y \in \mathbb{D}$.

□

Theorem 2 means we can judge if a ciphertext y is in the semi-order preserving set by checking if the interval $(P_{CY}(y-1), P_{CY}(y))$ is split by $P_{CX}(x)$. The reverse of Theorem 2 is also true.

Theorem 3. *Assume f: $X \to Y$ is a SOPE and $y \in \mathbb{Y}$. If there exist 2 plaintext $x_1 < x_2$ and $P_{X,Y}(x_1, y) > 0$, $P_{X,Y}(x_2, y) > 0$, then*

$$P_{CY}(y-1) < P_{CX}(x_1) \le P_{CX}(x_2-1) < P_{CY}(y), \tag{46}$$

Proof. We prove the theorem by contradiction. Assume

$$P_{CX}(x_1) \le P_{CY}(y-1), \tag{47}$$

thus,

$$P_{CX}(x_1-1) \le P_{CX}(x_1) \le P_{CY}(y-1) \le P_{CY}(y-1), \tag{48}$$

and

$$\|[P_{CX}(x-1), P_{CX}(x)] \cap [P_{CY}(y-1), P_{CY}(y)]\| = 0. \tag{49}$$

According to Corollary 1, this means $P_{X,Y}(x_1, y) = 0$, which contradicts with the condition $P_{X,Y}(x_1, y) > 0$. Thus $P_{CX}(x_1) > P_{CY}(y-1)$.

Similarly, we have $P_{CX}(x_2) < P_{CY}(y)$; thus, the theorem is proved. □

Theorem 3 gives the property of ciphertexts in the semi-order preserving set. If $y \in \mathbb{D}$, there will be a plaintext cumulative distribution value in the interval $(P_{CY}(y-1), P_{CY}(y))$.

3.2. Relationship between semi-order preserving degree and ciphertext expansion

Ciphertext expansion R_e is defined as the ratio of the size of ciphertext space to the size of plaintext space, i.e.,

$$R_e = \|\mathbb{Y}\|/\|\mathbb{X}\| = M/N. \tag{50}$$

Because a ciphertext in the semi-order preserving set corresponds to multiple plaintexts, we may guess that R_e decreases when d increases. Below we show the relationship between d and R_e.

Theorem 4. *If f: $X \to Y$ is a SOPE, then*

$$R_e \le \frac{1}{d}, \tag{51}$$

where $R_e = M/N$ is the ciphertext expansion and d is the semi-order preserving degree defined in Eq. (33).

Proof. In our scenario, the ciphertext follows a uniform distribution; thus,

$$P_\infty(X|Y) = \frac{1}{M}\sum_y \max_x P_{X|Y}(x,y). \tag{52}$$

We use a function $sp(y)$ to denote the size of preimage of y, i.e.,

$$sp(y) = \|\{x|P_{X,Y}(x,y) > 0\}\|. \tag{53}$$

Because the ciphertext follows a uniform distribution, we have $g(y) \ge 1$ for every ciphertext y. We then can divide the ciphertexts into three parts, $sp(y) = 1$, $sp(y) = 2$ and $sp(y) \ge 3$. For each ciphertext y, we define three random variables corresponding to the three possibilities:

$$[g_1(y), g_2(y), g_3(y)] = \begin{cases} [1,0,0], & sp(y) = 1 \\ [0,1,0], & sp(y) = 2 \\ [0,0,1]. & sp(y) \ge 3 \end{cases} \tag{54}$$

For every y, one of $g_1(y)$, $g_2(y)$ and $g_3(y)$ will be 1 and the other two will be 0. Thus,

$$\begin{aligned} \sum_y P_Y(y)(g_1(y) + g_2(y) + g_3(y)) &= \sum_y P_Y(y) \\ &= 1. \end{aligned} \tag{55}$$

When $g_2(y) = 1$, there exist two plaintexts, x_1, x_2, with $x_1 < x_2$ such that $P_{X,Y}(x_1, y) > 0$ and $P_{X,Y}(x_2, y) > 0$. According to Theorem 3, we have $P_{CX}(x_1) \in (P_{CY}(y-1), P_{CY}(y))$.

When $g_3(y) = 1$, there exist three plaintexts, $x_1 < x_2 < x_3$, such that $P_{X,Y}(x_i, y) > 0$ for $i = 1, 2, 3$. According to Theorem 3, we have $P_{CX}(x_1), P_{CX}(x_2) \in (P_{CY}(y-1), P_{CY}(y))$.

Thus,

$$\|\{P_{CX}(x_i)\} \cap (P_{CY}(y-1), P_{CY}(y))\| \ge g_2(y) + 2g_3(y), \tag{56}$$

and

$$\begin{aligned} \sum_y (g_1(y) + 2g_2(y)) &\le \|\{P_{CX}(x_i)\} \cap [0,1]\| \\ &\le \|\{P_{CX}(x_i)\}\| \\ &= N. \end{aligned} \tag{57}$$

If $y \in D$, then $g_2(y) = 1$ or $g_3(y) = 1$; thus, the semi-order preserving degree can be expressed as

$$\begin{aligned} d &= \sum_y P_Y(y)(g_2(y) + g_3(y)) \\ &= \sum_y \frac{1}{M}(g_2(y) + g_3(y)) \\ &\le \frac{1}{M}\sum_y (g_2(y) + 2g_3(y)) \\ &\le \frac{N}{M} \\ &= \frac{1}{R_e}. \end{aligned} \tag{58}$$

This is equivalent to

$$R_e \le \frac{1}{d}. \tag{59}$$

□

Theorem 4 shows the restrictions on the ciphertext expansion and semi-order preserving degree. Reduction of ciphertext expansion R_e can be realized by increasing d.

3.3. Relationship between semi-order preserving degree and security

We adopt min-entropy [25] to measure the SOPE security. The min-entropy of X is defined as

$$H_\infty(X) = -\log \max_x Pr[X = x]. \tag{60}$$

The average min-entropy of X conditioned on Y is

$$H_\infty(X|Y) = -\log \sum_y P_Y(y) \max_x P_{X|Y}(x, y). \tag{61}$$

The average min-entropy $H_\infty(X|Y)$ is equivalent to the average maximum likelihood $P_\infty(X|Y)$, which is defined as

$$\begin{aligned} P_\infty(X|Y) &= e^{-H_\infty(X|Y)} \\ &= \sum_y P_Y(y) \max_x P_{X|Y}(x, y). \end{aligned} \tag{62}$$

For convenience, we will use $P_\infty(X|Y)$ to indicate the security.

We discuss the security of SOPE under a known background model, in which the adversary knows the plaintext distribution P_X as well as the ciphertext sequence. In such circumstance, the average min-entropy of plaintext X conditioned on ciphertext Y, $H(X|Y)$ measures the leakage-resilient degree of SOPE. Note the adversary knows not only the ciphertext sequence but also the plaintext distribution P_X. However, the plaintext distribution is always uniform distribution in this paper, so P_X is omitted in the definition for convenience. This paper does not take the leakage of search or access patterns into consideration. Pseudo queries [22], private information retrieval [19], and Oblivious RAM [7] can be used to protect search and access patterns as necessary.

Below we show the relationship between the semi-order preserving degree d and security $P_\infty(X|Y)$.

Theorem 5. *For a SOPE f: $X \to Y$,*

$$P_\infty(X|Y) \ge 1 - d, \tag{63}$$

where $P_\infty(X|Y)$ is the average maximum likelihood defined in Eq. (62), and d is the semi-order preserving degree defined in Eq. (33).

Proof. Using notation defined in the proof of Theorem 4, $P_\infty(X|Y)$ can be estimated. If $g_1(y) = 1$, $\max_x P_{X|Y}(x, y) = 1$. If $g_2(y) = 1$, $\max_x P_{X|Y}(x, y) \ge 1/2$. If $g_3(y) = 1$, $\max_x P_{X|Y}(x, y) \ge 0$. Then $\max_x P_{X|Y}(x, y)$ satisfies:

$$\begin{aligned} \max_x P(x|y) &= (g_1(y) + g_2(y) + g_3(y)) \max_x P(x|y) \\ &= g_1(y) \max_x P(x|y) + g_2(y) \max_x P(x|y) + g_3(y) \max_x P(x|y) \\ &\ge g_1(y) + \frac{1}{2} g_2(y) \\ &= (g_1(y) + g_2(y) + g_3(y)) - \frac{1}{2}(g_2(y) + 2g_3(y)). \end{aligned} \tag{64}$$

We have

$$\begin{aligned} P_\infty(X|Y) &= \sum_y P_Y(y) \max_x P(x|y) \\ &= \frac{1}{M} \sum_y \max_x P(x|y) \\ &\ge \frac{1}{M} \sum_y (g_1(y) + g_2(y) + g_3(y)) - \frac{1}{2M} \sum_y (g_2(y) + 2g_3(y)) \\ &\ge 1 - \frac{N}{2M}. \end{aligned} \tag{65}$$

The relationship between the security $P_\infty(X|Y)$ and semi-order preserving degree d is

$$\begin{aligned} P_\infty(X|Y) &\geq \frac{1}{M}\sum_y (g_1(y)+g_2(y)+g_3(y)) - \frac{1}{2M}\sum_y (g_2(y)+2g_3(y)) \\ &\geq \frac{1}{M}\sum_y (g_1(y)+g_2(y)+g_3(y)) - \frac{1}{M}\sum_y (g_2(y)+g_3(y)) \\ &= 1-d. \end{aligned} \quad \square \tag{66}$$

Theorem 5 shows the restrictions on the security and semi-order preserving degree. When d decreases, SOPE becomes more vulnerable. If $d=0$, SOPE degenerates to OPE and $P_\infty(X|Y)=1$, which means that OPE scheme is insecure when the plaintext distribution is leaked.

3.4. Relationship between semi-order preserving degree and precision

Precision varies with applications. The main application of OPE-like methods is comparison of ciphertexts; thus, the precision of SOPE can be measured by the error rate of order relationship.

The difference between OPE and SOPE is that if $y_1 = y_2$ is possible when $x_1 \neq x_2$, $y_1 = Enc(x_1)$, $y_2 = Enc(x_2)$. We define the error rate as

$$P_e = P((x_1 \neq x_2) \wedge (y_1 = y_2)), \tag{67}$$

where x_1, y_1 and x_2, y_2 are 2 plaintext–ciphertext pairs.

Now we discuss the relationship between P_e and d. OPE is fully accurate in our precision definition, so $P_e = 0$ when $d = 0$. With the increase of d, P_e will also increase. Below we show the relationship between d and the error rate P_e.

Theorem 6. *For a SOPE f: $X \to Y$,*

$$P_e \leq \frac{1}{M}d, \tag{68}$$

where P_e is the error rate defined in Eq. (67), and d is the semi-order preserving degree defined in Eq. (33).

Proof. We have

$$\begin{aligned} P_e &= P((x_1 \neq x_2) \wedge (y_1 = y_2)) \\ &= \sum_y P((x_1 \neq x_2) \wedge (y_1 = y_2 = y)) \\ &= \sum_y P(x_1 \neq x_2 | y_1 = y_2 = y) P(y_1 = y_2 = y) \\ &= \sum_y P_{ey}(y) P(y_1 = y_2 = y) \\ &= \sum_y P_{ey}(y) P(y_1 = y | y_2 = y) P(y_2 = y) \\ &= \sum_y \frac{1}{M^2} P_{ey}(y) \\ &= \frac{1}{M^2}\sum_y P_{ey}(y), \end{aligned} \tag{69}$$

where $P_{ey}(y) = P(x_1 \neq x_2 | y_1 = y_2 = y)$.

We can split P_e to different cases as before. When $g_1(y) = 1$, $P_{ey}(y) = 0$. When $g_2(y) = 1$, 2 plaintexts are mapped to y. Denote them as y' and y''. Then $P_{ey}(y) = 2P(x'|y)P(x''|y)$. Considering that $P(x'|y) + P(x''|y) = 1$, we have $P_{ey}(y) \leq 1/2$. When $g_3(y) = 1$, $P_{ey}(y) \leq 1$.

In summary,

$$P_e \leq (1/2)g_2(y) + g_3(y). \tag{70}$$

Thus,

$$\begin{aligned} P_e &= \frac{1}{M^2}\sum_y P_{ey}(y) \\ &\leq \frac{1}{M^2}\sum_y \left(\frac{1}{2}g_2(y) + g_3(y)\right) \\ &\leq \frac{1}{2M^2}N. \end{aligned} \tag{71}$$

The relationship between the precision P_e and the semi-order preserving degree d is

$$\begin{aligned} P_e &\le \frac{1}{M^2}\sum_y (\frac{1}{2}g_2(y)+g_3(y)) \\ &\le \frac{1}{M^2}\sum_y (g_2(y)+g_3(y)) \\ &= \frac{1}{M}d. \end{aligned} \quad \square \tag{72}$$

Theorem 6 means that the semi-order preserving degree provides an upper limit for the error rate; thus, we can reduce the error rate and improve precision by lowering d. However, as shown in Theorems 4 and 5, the decrease of d will lead to larger ciphertext expansion and lower security. Thus, a SOPE user needs to face the trade-off and can strike a balance among ciphertext expansion, security, and precision by adjusting the semi-order preserving degree.

Note that in the scenario of ciphertext range query, which is the most frequently discussed situation for OPE, a SOPE user can get the same precision as OPE with some communication and calculation cost, if desired. For plaintext query $[x_1, x_2]$, if we generate ciphertext query $[y_1, y_2]$, where $y_1 = \min_y\{y|P_{X,Y}(x_1, y)\} > 0$ and $y_1 = \max_y\{y|P_{X,Y}(x_2, y)\} > 0$, then the range query on ciphertext will return all related results with some unrelated results, and the user can filter unrelated results after decryption.

4. SOPE construction

In this section, we propose a construction of the SOPE scheme. The proposed scheme takes a plaintext sequence x^n and an expected semi-order degree d_0 as input; it then generates a ciphertext sequence that follows a uniform distribution as output, and the actual semi-order degree d is close to d_0.

4.1. Implementation with real numbers

The size of ciphertext space can be calculated based on Theorem 3 with P_X and d_0.

Unlike OPE, SOPE may encrypt different plaintext symbols to the same ciphertext symbol, thus, the ciphertext sequence cannot be decrypted merely with the mapping from the plaintext space to the ciphertext space.

To solve this problem, the proposed encryption procedure maintains an inner state v_i, which will be used in the decryption procedure to recover the plaintext sequence.

In the first step, v_1 is randomly chosen from the interval $(P_{CX}(x_1-1), P_{CX}(x_1))$.

In the i-th encryption step, v_i and y_i are generated using x_i, y_{i-1} and v_{i-1}. v_i is generated by a linear transformation from $[P_Y(y-1), P_Y(y)]$ to $[P_X(x-1), P_X(x)]$ as

$$v_i = \frac{P_X(x_i)}{P_Y(y_{i-1})}(v_{i-1} - P_{CY}(y_{i-1}-1)) + P_{CX}(x_i-1), \tag{73}$$

and y_i is chosen such that $P_{CY}(y_i-1) \le v_i < P_{CY}(y_i)$. It is obvious that y_i is uniquely determined by v_i.

At the last step of the encryption, the value v^n is recorded as the decryption key.

The decryption is the reverse of the encryption procedure. v_i can be calculated from x_{i+1}, y_i and v_{i+1} as

$$v_{i-1} = \frac{P_Y(y_{i-1})}{P_X(x_i)}(v_i - P_{CX}(x_i-1)) + P_{CY}(y_{i-1}-1), \tag{74}$$

and x_i can be determined by condition $P_{CX}(x_i-1) < v_i < P_{CX}(x_i)$.

4.2. Implementation with finite precision

However, implementation in the preceding subsection assumes infinite precision which is unfeasible in practice. In this subsection, we propose an implementation using real numbers with finite precision. A real number r with finite precision can be represented by an integer a with precision b as $r = a * 2^{-b}$.

In the ith step of the encryption, we use a pair of b-bit real numbers, v'_i and v''_i, to substitute the value v_i. The encryption and decryption procedures now become the transformation of 2 values. The encryption procedure now becomes

$$\begin{aligned} v'_i &= l_1(v'_{i-1}, x_i, y_{i-1}) \\ v''_i &= l_1(v''_{i-1}, x_i, y_{i-1}) \end{aligned} \tag{75}$$

where

$$l_1(v, x, y) = \frac{P_X(x)}{P_Y(y)}(v - P_Y(y-1)) + P_{CX}(x-1). \tag{76}$$

Table 2
Experiment results of $d_0 = 0.5, 0.4, 0.3, 0.25$.

Expected semi-order degree d_0	0.5	0.4	0.3	0.25
Actual semi-order degree d	0.503	0.414	0.312	0.240
Ciphertext expansion R_e	1.97	2.39	3.17	4.12
Average maximum likelihood P_∞	0.873	0.895	0.921	0.939
Error rate P_e	0.00502	0.00417	0.00315	0.00238

The reverse of encryption iteration l_1 is

$$l_2(v, x, y) = \frac{P_Y(y)}{P_X(x)}(v - P_X(x-1)) + P_{CY}(y-1) \tag{77}$$

From the $(i-1)$-th step to the ith step, v needs to satisfy following conditions:

1. Encryption should ensure $v_i'' > v_i'$. If $v_i' = v_i''$; no further encryption is possible.
2. Encryption should ensure v_i', v_i'' correspond to a unique ciphertext y. If there are multiple y, the decryption procedure will be ambiguous.
3. Encryption should ensure $v_{i-1}' \le l_2(v_i', x_i, y_{i-1})$ and $l_2(v_i'', x_i, y_{i-1}) \le v_{i-1}''$. This guarantees the decryption to be in the same range as in the encryption.

To guarantee the three conditions, we make precision b changeable throughout the encryption procedure.

When one of the three conditions is violated, precision is increased by one, i.e., $b \leftarrow b+1$, and half of $[v', v'']$ is set as new $[v', v'']$, i.e.,

$$\begin{aligned} v' &\leftarrow v', \\ v'' &\leftarrow \frac{1}{2}(v' + v''), \end{aligned} \tag{78}$$

or

$$\begin{aligned} v' &\leftarrow \frac{1}{2}(v' + v''), \\ v'' &\leftarrow v'', \end{aligned} \tag{79}$$

until the three conditions above are satisfied.

At the last step of encryption, we record $v_n = v_n'$ as the decryption key. The decryption starts from v_n. x_k, and v_{k-1} can be recovered from v_k and y_{k-1}. x_k should satisfy $P_{CX}(x_k - 1) < v_k < P_{CX}(x_k)$, and x satisfying such a condition is unique. v_{k-1} can be calculated by

$$v_{k-1} = l_2(v_k, x_k, y_{k-1}). \tag{80}$$

According to the encryption procedure, if $v_k' \le v_k \le v_k''$, then

$$v_{k-1}' \le l_2(v_k', x_k, y_{k-1}) \le g_2(v_k, x_k, y_{k-1}) = v_{k-1}, \tag{81}$$

and

$$v_{k-1}'' \ge l_2(v_k'', x_k, y_{k-1}) \ge g_2(v_k, x_k, y_{k-1}) = v_{k-1}, \tag{82}$$

i.e.,

$$v_{k-1}' \le v_{k-1} \le v_{k-1}''. \tag{83}$$

Thus the plaintext sequence can be fully decrypted without errors.

The detailed encryption and decryption procedures are shown in Algorithms 1 and 2.

4.3. Performance

We use an experiment to show the performance of the proposed scheme. The plaintext sequence x^n follows a uniform distribution on [1, 100], and the length of the plaintext sequence is 5000. The proposed implementation is run four times with $d_0 = 0.5, 0.4, 0.3, 0.25$, respectively, and a plaintext sequence of length 5000 is generated each time. The results are shown in Table 2.

The simulation results of the proposed scheme behaves as expected. With the decrease of d_0, the system will have a larger ciphertext expansion R_e, larger average maximum likelihood P_∞, and lower error rate P_e. Thus, the user can adjust d_0 to get the balance among the ciphertext expansion, security, and error rate.

Algorithm 1 Encryption.

Input

Plaintext sequence (x_i), i=1, 2, ... , n.,
Plaintext distribution P_X, expected semi-order degree d_0.

Output

Ciphertext sequence (y_i), i=1, 2, ... , n., decryption key v_n

Function *Encrypt*

$P_Y \leftarrow FindP_Y(P_X, d)$
Randomly select v'_1, v''_2 such that
  $P_{CX}(x_1 - 1) < v' < v'' < P_{CX}(x_1)$ with precision bit b.
  There exists y with $P_{CX}(y-1) < v' < v'' < P_{CX}(y)$.
$y_1 \leftarrow y$
For $i = 2$ to n
  $v'_i = l_1(v'_{i-1}, x_i, y_{i-1})$
  $v''_i = l_1(v''_{i-1}, x_i, y_{i-1})$
  $k \leftarrow 1$
  While $Verify(v', v'', x_i, y_{i-1})$ is False:
    $b \leftarrow b + 1$, $k \leftarrow k + 1$
    Re-calculate v'_i, v''_i with precision bit b
    Equally split $[v'_i, v''_i]$ to 2^k parts, and randomly choose 1 $[u', u'']$
    $v'_i, v''_i \leftarrow u', u''$
  Find y with $P_{CX}(y-1) < v'_i < v''_i < P_{CX}(y)$
  $y_i \leftarrow y$
Return (y_i), v_n.

Function $FindP_Y(P_X, d)$

$n_x \leftarrow |P_X|$
$n_y \leftarrow \lfloor n_x/d * (1 + Random(-0.05, 0.05)) \rfloor$
$P_Y \leftarrow Uniform(\{1, 2, \ldots, n_y\})$
return P_Y

Function $Verify(v'_i, v''_i, x_i, y_{i-1})$:

If $(v' >= v'')$ return False
If there exists y such that $(v'_i < P_{CY}(y) < v''_i)$ return False
If $v'_{i-1} > l_2(v'_i, x_i, y_{i-1})$ return False
If $l_2(v''_i, x_i, y_{i-1}) > v''_{i-1}$ return False
Return True

Algorithm 2 Decryption step.

Input

Ciphertext sequence (y_i), i=1, 2, ... , n., decryption key v_n,
Plaintext distribution P_X, ciphertext distribution P_Y.

Output

Plaintext sequence (x_i), i=1, 2, ... , n.

Function *Decryption*

For $k = n$ to 1:
  Find x satisfies $P_{CX}(x-1) < v_k < P_{CX}(x)$
  $x_k \leftarrow x$
  $v_{k-1} = l_2(v_k, x_k, y_{k-1})$
Return (x_i)

5. Conclusion

In this paper, we proposed SOPE, a new primitive to support searching on ciphertext. We then studied the security, precision, and ciphertext expansion of SOPE. With the help of semi-order preserving degree d, the performance of SOPE can be adjusted according to different situations. At last, we proposed an implementation of SOPE.

Acknowledgments

This work was supported in part by the Natural Science Foundation of China under Grant U1636201, 61572452, 61502007 and U1536108, in part by the China Postdoctoral Science Foundation under Grant 2015M582015, and in part by the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06030601.

References

[1] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, Order preserving encryption for numeric data, in: Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data, SIGMOD '04, ACM, New York, NY, USA, 2004, pp. 563–574.
[2] M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: opportunities and challenges, Inf. Sci. 305 (2015) 357–383.
[3] A. Boldyreva, N. Chenette, Y. Lee, A.O. Neill, Order-preserving symmetric encryption, in: A. Joux (Ed.), Advances in Cryptology – EUROCRYPT 2009, Vol. 5479 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 224–241.
[4] A. Boldyreva, N. Chenette, A.O. Neill, Order-preserving encryption revisited: improved security analysis and alternative solutions, in: P. Rogaway (Ed.), Advances in Cryptology C CRYPTO 2011, Vol. 6841 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2011, pp. 578–595.
[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, Public key encryption with keyword search, in: C. Cachin, J. Camenisch (Eds.), Advances in Cryptology – EUROCRYPT 2004, Vol. 3027 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2004, pp. 506–522.
[6] Y.-C. Chen, C. Lee, The σ-neighborhood skyline queries, Inf. Sci. 322 (2015) 92–114.
[7] C. Fletcher, M. Naveed, L. Ren, E. Shi, E. Stefanov, Bucket ORAM: single online roundtrip, constant bandwidth oblivious RAM, Tech. rep., IACR Cryptology ePrint Archive, 2015. Report 2015, 1065
[8] Z. Fu, K. Ren, J. Shu, X. Sun, F. Huang, Enabling personalized search over encrypted outsourced data with efficiency improvement, IEEE Trans. Parallel Distrib. Syst. 27 (9) (2016) 2546–2559.
[9] C. Gentry, Fully homomorphic encryption using ideal lattices, in: Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing, STOC 09, ACM, New York, NY, USA, 2009, pp. 169–178.
[10] E.-J. Goh, 2003, Secure indexes, Cryptology ePrint Archive, Report 2003/216, http://eprint.iacr.org/2003/216/.
[11] 2015, Google, The encrypted bigquery client, https://github.com/google/encrypted-bigquery-client.
[12] S.F. Krendelev, M. Yakovlev, M. Usoltseva, Order-preserving encryption schemes based on arithmetic coding and matrices, in: Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on, vol. 480, 2014, pp. 891–899.
[13] K. Li, W. Zhang, C. Yang, N. Yu, Security analysis on one-to-many order preserving encryption-based cloud data search, IEEE Trans. Inf. Forensics Secur. 10 (9) (2015) 1918–1926.
[14] S. Martınez, J.M. Miret, R. Tomas, M. Valls, Securing databases by using diagonal-based order preserving symmetric encryption, Appl. Math. Inf. Sci. 8 (5) (2014) 2085.
[15] M. Naveed, S. Kamara, C.V. Wright, Inference attacks on property-preserving encrypted databases, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS 15, ACM, New York, NY, USA, 2015, pp. 644–655.
[16] R.A. Popa, C.M.S. Redfield, N. Zeldovich, H. Balakrishnan, Cryptdb: protecting confidentiality with encrypted query processing, in: Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, SOSP 11, ACM, New York, NY, USA, 2011, pp. 85–100.
[17] R. Popa, F. Li, N. Zeldovich, An ideal-security protocol for order-preserving encoding, in: Security and Privacy (SP), 2013 IEEE Symposium on, vol. 465, 2013, pp. 463–477.
[18] D.X. Song, D. Wagner, A. Perrig, Practical techniques for searches on encrypted data, in: Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on, 2000, pp. 44–55.
[19] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, R. Buyya, Ensuring security and privacy preservation for cloud data services, ACM Comput. Surv. 49 (1) (2016) 13:1–13:39.
[20] C. Wang, N. Cao, K. Ren, W. Lou, Enabling secure and efficient ranked keyword search over outsourced cloud data, IEEE Trans. Parallel Distrib. Syst. 23 (8) (2012) 1467–1479.
[21] S. Wozniak, M. Rossberg, S. Grau, A. Alshawish, G. Schaefer, Beyond the ideal object: towards disclosure-resilient order-preserving encryption schemes, in: Proceedings of the 2013 ACM Workshop on Cloud Computing Security Workshop, CCSW 13, ACM, New York, NY, USA, 2013, pp. 89–100.
[22] Z. Wu, J. Shi, C. Lu, E. Chen, G. Xu, G. Li, S. Xie, P.S. Yu, Constructing plausible innocuous pseudo queries to protect user query intention, Inf. Sci. 325 (2015) 215–226.
[23] Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst. 27 (2) (2016) 340–352.
[24] T. Xiang, X. Li, F. Chen, S. Guo, Y. Yang, Processing secure, verifiable and efficient SQL over outsourced database, Inf. Sci. 348 (2016) 163–178.
[25] L. Xiao, I.-L. Yen, Security analysis for order preserving encryption schemes, in: Information Sciences and Systems (CISS), 2012 46th Annual Conference on, 2012, pp. 1–6.