Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Towards optimal noise distribution for privacy preserving in data aggregation

Hao Zhang [a], Nenghai Yu [a,*], Yonggang Wen [b], Weiming Zhang [a]

[a] Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei 230027, China

[b] School of Computer Engineering, Nanyang Technological University, 639798 Singapore

ARTICLE INFO

Article history:
Received 28 November 2013
Received in revised form
22 March 2014
Accepted 25 May 2014
Available online 4 June 2014

Keywords:
Aggregation
Privacy protection
Noise addition
Mutual information
Gaussian distribution

ABSTRACT

In aggregation applications, individual privacy is a crucial factor to determine the effectiveness, for which the noise-addition method (i.e., a random noise value is added to the true value) is a simple yet powerful approach. However, improper additive noise could result in bias for the aggregate result. It demands an optimal noise distribution to reduce the deviation. In this paper, we develop a mathematical framework to derive the optimal noise distribution that provides privacy protection under the constraint of a limited value deviation. Specifically, we first derive a generic system dynamic function that the optimal noise distribution must satisfy, and further investigate the special case that the original values obey Gaussian distribution. Then we detailedly investigate the general cases that the original values obey arbitrary continuous distribution, which can be expressed by Gaussian Mixture Model (GMM). Our theoretical analysis suggests that for the Gaussian input Gaussian distribution is the optimal solution, and for the general input, the optimal solution is composed of infinite number of Gaussian components. We further find the general term formula of the components, which reduces the number of unknowns from infinite to three, i.e. the parameters of the first component (variance, expectation, weight). Based on it, we investigate the properties and propose an algorithm in order to calculate the asymptotically optimal solution composed of finite Gaussian components. The numerical evaluation shows that the results has little deviation to the optimal solutions.

1. Introduction

With the advance of information age, data aggregation has been widely used in daily life and commercial applications. Even some companies such as Canalys make a living by providing all kinds of statistics. In aggregation applications the server wishes to distill valuable aggregate statistics from a mass of individual data. For example, CarTel (Hull et al., 2006) learns the traffic condition from the road information collected by using mobile phones. BikeNet (Eisenman et al., 2009) measures air and road condition to guide cyclists, where all the data is contributed by users' devices.

However, the individual privacy may be violated during the aggregation. The server is able to obtain the individual data of participants from inputs. Nevertheless, much of this information is private for individuals, such as health condition,

* Corresponding author.
E-mail addresses: zhh1000@mail.ustc.edu.cn (H. Zhang), ynh@ustc.edu.cn (N. Yu), ygwen@ntu.edu.sg (Y. Wen), zhangwm@ustc.edu.cn (W. Zhang).
http://dx.doi.org/10.1016/j.cose.2014.05.009
0167-4048/

income, etc., especially in the presence of curious server or data abuse. Actually the server only need to know the aggregate result without knowing the individual data. Thus in aggregation applications, calculate the aggregate statistics without compromising individual privacy is an important challenge.

Some methods are proposed to solve this problem. Secure Multiparty Computation (SMC) is a good choice to calculate the statistics. It uses cryptographic methods, doing operations on ciphertext domain. However, it also has its limitations. Firstly, because of the huge overhead, SMC is not suitable for large-scale systems. Secondly, both encryption/decryption and communication are high power consumption operations, which limit SMC deployed in energy-sensitive devices (e.g. sensor, phone). Therefore, SMC is not suitable for the large-scale energy-constraint environments such as large-scale mobile survey applications. On the contrary, noise addition, which prevents the adversary from getting the accurate individual data values, is a simple but effective method. Compared to SMC, it is much simpler and efficient, especially in this environment. Without collaboration with others, each participant only adds noise into his data independently before updating. However, in this method, how to choose the noise distribution is a headache. Improper additive noise could result in bias for the aggregate result. It demands an optimal noise distribution which provides the best protection to individual privacy while the aggregate result has tolerable bias. However, the optimal noise distribution is not evident. Usually the noise distribution (usually homogeneous noise or Gaussian noise) is proposed directly without any explanation.

In aggregation applications the accuracy of result and the privacy of individuals are two main concerned issues. Our goal is to find out the optimal noise distribution in noise addition method, where the individual privacy is protected best under the given accuracy requirement. In this paper, we measure the accuracy by expectation and variance of the noise distribution, and the privacy by conditional entropy. Based on the metrics, we develop a mathematical framework to derive the optimal noise distribution that provides privacy protection under the constraint of a limited value deviation, deriving a generic system dynamic function that the optimal noise distribution must satisfy, with the original data distribution as input. Based on the function, we first investigate the special case for Gaussian input, then the arbitrary input is considered and analyzed intensively. The contributions of this paper are summarized as follows:

1. Based on the accuracy and privacy metrics, we develop a mathematical framework to derive the optimal noise distribution.
2. We get the generic system dynamic function that the optimal noise distribution must satisfy, where the input is the distribution of original individual data. Based on the function, we find Gaussian distribution is the optimal noise distribution for the Gaussian input.
3. We deeply investigate the general case that the input is arbitrary continuous distribution. We propose a general method to calculate the optimal noise distribution.
4. We investigate the properties of the optimal noise distribution, which is composed of infinite Gaussian components, and find the periodic structure so that it can be approximated by finite components.
5. We propose an algorithm calculating the optimal distribution. For some special cases, the complexity of the algorithm is reduced greatly, and the approximation matches the theoretic analysis well.

The rest of the paper are organized as follows. Related work is introduced in Section 2. We formulate the problem in Section 3. In Section 4 we give the general solution and investigate the Gaussian input. Arbitrary continuous distribution input is explored in Section 5, and we find out that output consists of infinite Gaussian components, all of which are fixed by the first component. In Section 6 we investigate the properties of the component sequence. In Section 7 we propose an algorithm to express the approximate optimal distribution, and reducing the algorithm complexity in two special cases. Section 8 shows some simulation results. At last we conclude the paper and the future work in Section 9.

2. Related work

SMC enables parties to calculate the result by collaboration based on their own data without compromising others' privacy. However it has lots of limitations. In Clifton et al. (2002) a secure sum protocol was depicted, where the summation is calculated serially which would spend too much time in large-scale systems. Another protocol (Shi et al., 2011) was proposed, which allows the untrusted server to calculate the summation. It requires that the sum of the keys of parties is 0. If one of the party leaves in the process, which is a common case in large-scale systems, the summation cannot be calculated. Jung et al. (2013) proposed a linear time protocol without secure channel, but it still needs lots of communications among parties. Meanwhile, in these methods each party has to communicate with others and do lots of mathematical operations, both of which are high power consumption operations. So SMC is not suitable for energy-constrained devices.

Noise addition has been studied for many years in secure data mining (Adam and Worthmann, 1989). It prevents the adversary from getting the accurate individual data values. Plenty of schemes are proposed to preserve the privacy of individual records, but they all do not solve the problem as ours. Most of them such as Oliveira and Zaiane (2003); Su et al. (2008) are not claimed whether their methods are optimal. Furthermore, they utilize the covariance of data in the database, which needs the party who adds the noise to know the global information of data. In some schemes the noise is added without concerning the covariance of the data, but the uniform distribution or Gaussian distribution is directly declared (Agrawal and Srikant, 2000; Domingo-Ferrer et al., 2004). In Zhu and Liu (2004) the authors considered the optimal randomization given the bias of results, but they did not solve it. Traub et al. (1984) analyzed the tradeoff of the magnitude of the perturbations and the error Chebyshevs inequality, but the metrics are rough. Different from many other researches, Dwork et al. (2006) proposed a method that the bias of summation obeys specified distribution. It adds

noise into the summation directly, which is different from other works focussing on adding noises into individual values. Meanwhile, some researchers (Agrawal and Srikant, 2000; Agrawal and Aggarwal, 2001) found the original data distribution can be restructured by perturbed values, but the individual privacy is not violated yet.

To protect the privacy of individual data, the privacy metric is necessary and has greatly influence on the protection scheme. There are several different measures of privacy. In Agrawal and Srikant (2000) the privacy is measured by "confidence interval". If the data concerned x is in the interval $I(x)$ with at least certain probability c%, the length of interval $|I(x)|$ is treated as a privacy measure. However, this measure is not accurate. Mutual information or differential entropy in Shannon's information theory is another much more popular privacy metric (Agrawal and Aggarwal, 2001). It indicates the average privacy supporting by mathematical theory. Renyi entropy (an extension of Shannon entropy) is also used to measure privacy (Rachlin et al., 2009), but it is too complex and does not have obvious physical meaning. Besides, some privacy metrics for single record are proposed in Bezzi (2010), which are also based on Shannon entropy.

Recent years differential privacy (Dwork, 2006) is a hot noise addition technology protecting individual's privacy in data mining. It guarantees the accuracy of statistical result while avoiding individual record disclosure. Ghosh et al. (2009, 2011) find out the optimized noise distribution that provides most accurate result under the given privacy requirement. However, differential privacy is against the adversary that obtains individual record from different statistic results. For example, if A is the sum of 50 records, B is the sum of 49 records from the former 50 ones. One record is disclosed by $A - B$. In our situation, the adversary can get the individual records directly, and we only focus on one aggregation process.

3. Problem formulation

In this section, firstly we introduce some aggregation applications where the violation of individual privacy potentially exists and noise addition method is appropriate. Then we quantify the accuracy and privacy requirements. Finally, based on the measurements the optimization problem is presented.

3.1. Applications

The individual privacy is potentially threatened in statistics aggregation applications. There are many examples, including:

- **Sensor network aggregation**. In sensor network applications, many energy-constrained sensors are widely deployed to monitor the surrounding environment and send data to the central server for aggregation. However, the data from individual sensor may contain privacy-sensitive information. So energy-efficient privacy protection in aggregation is an important issue.
- **Mobile survey applications**. In these applications, tens of thousands of participants exist and the phones are energy-constrained. The overall results are distilled from a large amount of individual information collected by mobile phones. However, the individual privacy may be violated during information collection.

In these large-scale energy-constrained applications, the server should know is the aggregate results, which are distilled from the information of individuals. However, the individual privacy may be violated during the collection. Noise addition technology is a simple but efficient method in these applications, which protects the individual privacy by adding noise into the individual data. To describe the problem more accurately, in the following we formulate the problem in the mathematical way.

3.2. Accuracy and privacy measurement

Suppose there are n users with values x_i, $i = 1, 2, \ldots, n$, and a server calculating aggregate statistics. In this paper, we mainly focus on a simple but common statistic problem called summation. The server processes the aggregation function $sum(v) = \sum_{i=1}^{n} x_i$. Of course there are several other aggregation types. Besides summation, Popa et al. (2011) list other classes: average, standard deviation, count and others. All of them can be constructed by summation.

To protect the individual privacy in the process of aggregating statistics, user u_i adds random *noise* z_i into his/her *true value* x_i. Instead of x_i, u_i contributes the *perturbed value* $y_i = x_i + z_i$ to the server. The information that the attacker knows most is all the perturbed values and the scheme by which the noise is generated. So we suppose the attacker knows y_i and the distributions of y_i and z_i. He tries to get x_i based on the information he knows. The aim of the noise is to prevent the attacker from getting the accurate true value.

Obviously different noise distributions have different privacy protection capability. To protect the true value, how to choose a good noise distribution is the key issue. Noise Z_i is a random variable with the probability density function (pdf) f_{Z_i}. To meet the requirements of accuracy and privacy, f_{Z_i} should satisfy:

1. accuracy requirement: the difference of $\sum Y_i$ and $\sum X_i$ is small.
2. privacy requirement: the confusion of the true value is evident.

The first requirement guarantees that the aggregate result does not deviate from the true result too much. The second one guarantees the individual privacy is not violated. If the attacker gets the user's value, he still doubts about it because of the existence of noise.

3.2.1. Accuracy measurement

For accuracy requirement, we define the difference

$$M_n = \sum_{i=1}^{n} Y_i - \sum_{i=1}^{n} X_i = \sum_{i=1}^{n} Z_i, \tag{1}$$

where n is the number of participants. Due to $Z_1, \ldots, Z_n$ are random variables, M_n also is a random variable, with the

expectation $E(M_n)$ and the variance $D(M_n)$. $Z_1, Z_2, \ldots, Z_n$ are independent, where Z_i has the expectation μ_{Z_i} and the variance $\sigma^2_{Z_i}$ respectively. If they satisfy Lindeberg's condition (Lindeberg), M_n obeys Gaussian distribution regardless of the distributions of individual noise. It is only decided by the expectation and the variance, i.e. $E(M_n) = \sum_{i=1}^{n} \mu_{Z_i}$, $D(M_n) = \sum_{i=1}^{n} \sigma^2_{Z_i}$. We try to keep M_n small with high probability. It requires $E(M_n) = 0$ and $D(M_n)$ is small. Therefore, we quantify the *accuracy requirement* U as

$$U = \frac{D(M_n)}{n} = \frac{1}{n}\sum_{i=1}^{n} \sigma^2_{Z_i} \tag{2}$$

with an additional condition $E(M_n) = 0$. It measures the average deviation tolerance of the perturbed result from the true result. Suppose $Z_1, \ldots, Z_n$ are independent and identically distributed random variables with the expectation μ_Z and the variance σ^2_Z. The accuracy requirement U is simplified as

$$U = \sigma^2_Z \tag{3}$$

with $\mu_Z = 0$.

U measures the average deviation tolerance of the perturbed result from the true result by the variance of the noise distribution. If two zero-mean noise distribution f_{Z_i} and f_{Z_j} satisfy $U_i < U_j$, it means f_{Z_i} guarantees the accuracy of result better.

3.2.2. *Privacy measurement*

For privacy requirement, we should enlarge the uncertainty of the individual's value. Suppose $Z_1, \ldots, Z_n$ are independent and identically distributed random variables, denoted as Z. Consider

$$Y = X + Z \tag{4}$$

where Y, X and Z are random variables which delegate individual's perturbed value, true value and noise respectively, and Z is independent from X. Suppose the adversary knows the distribution of Z. It is reasonable that any user knows it to generate noise, including malicious user compromised by the adversary. For user u_i, because of the perturbation of noise z_i, the adversary is uncertain about x_i when he gets y_i. We use Shannon's information entropy to measure the uncertainty. Suppose the adversary gets y_i, the uncertainty of X is measured by $H(X|Y = y_i) = -\sum_x P_{X|Y}(x|y)\log P_{X|Y}(x|y)$. The larger $H(X|Y = y_i)$ is, the better the privacy protection is provided at y_i.

For different y_i, $H(X|Y = y_i)$ is different. we use the average $H(X|Y = y_i)$ to quantify the *privacy protection strength* (denoted by V) of the noise, i.e.

$$V = \sum_{y_i} H(X|Y = y_i)P_Y(y) = H(X|Y). \tag{5}$$

$H(X|Y)$ denotes the average uncertainty of the true value when the perturbed value is captured. The larger V is, the higher the average uncertainty is.

Generally speaking, for noise addition technology, the accuracy and the privacy are in contradiction. High accuracy leads to low privacy protection strength, and vice versa. However, for a given accuracy level, different f_Z usually has different privacy protection capability. Thus how to optimize the noise distribution that provides the best privacy protection under the accuracy constraint is the key problem.

3.3. *Optimization problem formulation*

For convenience, in the following we consider the continuous distributions. The discrete distribution can be regarded as the approximation of the corresponding continuous distribution. Consider the formulation $Y = X + Z$, where X, Z are random variables with pdf $f_x(x)$ and $f_Z(z)$ respectively. We will find the optimal f_Z providing the best privacy protection while guaranteeing that the result has an acceptable deviation, i.e.

$$\begin{aligned} \max_{f_Z(z)} \quad & V = H(X|Y) \\ \text{s.t.} \quad & U = \sigma^2_Z \le \sigma^2_m \\ & E(Z) = 0 \end{aligned} \tag{6}$$

where σ^2_m is the accuracy requirement bound required by applications.

Consider

$$H(X|Y) = H(X) - I(X;Y). \tag{7}$$

Since $f_x(x)$ is deterministic, $H(X)$ is a constant. Thus the optimization problem is translated to

$$\begin{aligned} \min_{f_Z(z)} \quad & I(X;Y) \\ \text{s.t.} \quad & \int f_Z(z)z^2\,dz \le \sigma^2_m \\ & \int f_Z(z)z\,dz = 0 \\ & \int f_Z(z)\,dz = 1. \end{aligned} \tag{8}$$

4. Problem solution

4.1. *General solution*

Consider the problem (8), for any pdf of X, we have the following theorem:

Theorem 1. *Given the accuracy requirement bound σ^2_m, the noise providing the best privacy protection has the pdf*

$$f_Z(z) = Cf_Y(z)e^{-\lambda z^2 - \omega z}, \tag{9}$$

where $f_Y(z) = \int f_x(x)f_Z(z - x)\,dx$, and λ, ω, C are related to the constraints $\int f_Z(z)z^2\,dz = \sigma^2_m$, $\int f_Z(z)z\,dz = 0$, and $\int f_Z(z)\,dz = 1$ respectively.

The proof is given in Appendix A.

Fig. 1 shows the corresponding system diagram, where f_x is the input and f_Z is the output. The system contains two operations. One is convolution of the input and the output. The other is multiplication of the convolution result and the factor "$C\,e^{-\lambda z^2 - \omega z}$".

The problem (8) is a convex optimization problem (Cover and Thomas, 2006). The constraints satisfy the sufficient

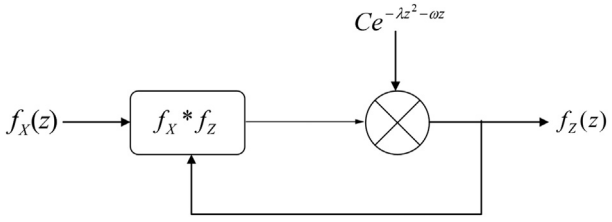

Fig. 1 – The system diagram.

conditions of KKT approach (inequality constraint is a continuously differentiable convex function, the equality constraints are affine functions (Hanson, 1999)). If we find one f_Z satisfying Eq. (9), it is the global optimal solution.

Here we have to know the distribution of the original data f_x as the input of the system. In practice, f_x can be estimated in several ways. The fist one is assuming f_x is a common distribution (e.g. Gaussian distribution). The second one is asking some statistics institutions the probable data distribution based on the similar application. The third one is sampling by adding specific noise such as Gaussian noise. Moreover, there may be many other better methods. Here we suppose f_x can be estimated. How to estimate f_x is beyond the scope of this paper.

4.2. *Gaussian distribution input*

Generally for different input $f_x(x)$, the output $f_Z(z)$ is different. We consider a special but popular case that X follows Gaussian distribution.

When $X \tilde{} N(\mu_X, \sigma_X^2)$, $Z \tilde{} N(0, \sigma_m^2)$ is a solution of Eq. (9), where

$$\lambda = \frac{1}{2}\left(\frac{1}{\sigma_m^2} - \frac{1}{\sigma_m^2 + \sigma_X^2}\right), \tag{10}$$

$$\omega = \frac{\mu_X}{\sigma_m^2 + \sigma_X^2} \tag{11}$$

$$C = \sqrt{\frac{\sigma_m^2}{\sigma_m^2 + \sigma_X^2}} \cdot e^{-\frac{\mu_X^2}{2\left(\sigma_m^2 + \sigma_X^2\right)}} \tag{12}$$

Thus $f_Z(z) = 1/\sigma_m \phi(z/\sigma_m)$ is the solution of the problem (8), where $\phi(x) = 1/\sqrt{2\pi}\, e^{-x^2/2}$. Therefore we have the theorem:

Theorem 2. *When X obeys Gaussian distribution, the noise which obeys Gaussian distribution with the expectation 0 and the variance σ_m^2 protects the individual privacy best.*

5. Gaussian mixture model input

For arbitrary f_x, the optimal f_Z satisfies Eq. (9). In the following, we formulate arbitrary f_x by Gaussian Mixture Model (GMM), and investigate the corresponding optimal noise distribution f_Z (in the following we denote the optimal noise distribution by f_Z).

5.1. *Solution translation*

From GMM, any continuous distribution can be approximated by the mixture of weighted Gaussian distributions, i.e. any continuous distribution f can be represented as

$$f(x) = \sum_{i=0}^{M-1} p_i g_i(x), \tag{13}$$

where p_i, $i = 0, \ldots, M-1$ ($M \in \mathbb{N}^+$), are the nonnegative mixture weights, and $g_i(x)$, $i = 0, \ldots, M-1$, are the Gaussian densities with expectation μ_i and expectation σ_i^2. The mixture weights satisfies $\sum_{i=0}^{M-1} p_i = 1$. Here we call $p_i g_i(x)$ Gaussian component, which is the product of Gaussian pdf and the weight. So the component is decided by three parameters (p_i, μ_i, σ_i^2). f is the merger of M Gaussian components, expressed as $f = (p_0 g_0(x), p_1 g_1(x), \ldots, p_{M-1} g_{M-1}(x))$.

Based on GMM, suppose f_x and f_Z consist of M Gaussian components and N ones respectively. They can be expressed by the merger of multiple Gaussian components, i.e.

$$f_X(x) = \frac{1}{\sqrt{2\pi}} \sum_{i=0}^{M-1} \frac{p_{X_i}}{\sigma_{X_i}} e^{-\frac{\left(x-\mu_{X_i}\right)^2}{2\sigma_{X_i}^2}} \tag{14}$$

$$f_Z(x) = \frac{1}{\sqrt{2\pi}} \sum_{j=0}^{N-1} \frac{p_{Z_j}}{\sigma_{Z_j}} e^{-\frac{\left(x-\mu_{Z_j}\right)^2}{2\sigma_{Z_j}^2}}. \tag{15}$$

A simpler expression is $f_x = (x_0, x_1, \ldots, x_{M-1})$, where x_i, $i = 0, \ldots, M-1$, is decided by the parameters $(p_{X_i}, \mu_{X_i}, \sigma_{X_i}^2)$ (denoted by $x_i = (p_{X_i}, \mu_{X_i}, \sigma_{X_i}^2)$), and $f_Z = (z_0, z_1, \ldots, z_{N-1})$ where z_j, $j = 0, \ldots, N-1$, is decided by $(p_{Z_j}, \mu_{Z_j}, \sigma_{Z_j}^2)(z_j = (p_{Z_j}, \mu_{Z_j}, \sigma_{Z_j}^2))$. In the following we consider the two operations of the system in Fig. 1.

5.1.1. *Convolution*

f_Y is the convolution of f_x and f_Z. According to the properties of convolution of Gaussian function,

$$f_Y(x) = \frac{1}{\sqrt{2\pi}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{p_{X_i} p_{Z_j}}{\sqrt{\sigma_{X_i}^2 + \sigma_{Z_j}^2}} e^{-\frac{\left(x-\mu_{X_i}-\mu_{Z_j}\right)^2}{2\left(\sigma_{X_i}^2+\sigma_{Z_j}^2\right)}}, \tag{16}$$

or $f_Y = (y_{00}, y_{01}, \ldots, y_{ji}, \ldots, y_{(N-1)(M-1)})$ where $y_{ji} = z_j^* x_i$ is a Gaussian component decided by $(p_{Y_{ji}}, \mu_{Y_{ji}}, \sigma_{Y_{ji}}^2)(y_{ji} = (p_{Y_{ji}}, \mu_{Y_{ji}}, \sigma_{Y_{ji}}^2))$, and $\mu_{Y_{ji}} = \mu_{Z_j} + \mu_{X_i}$, $\sigma_{Y_{ji}}^2 = \sigma_{Z_j}^2 + \sigma_{X_i}^2$, $p_{Y_{ji}} = p_{Z_j} p_{X_i}$. Each component of f_Z generates M component of f_Y. If f_Z is composed of N components, f_Y is composed of $M \cdot N$ components.

5.1.2. *Multiplication*

From the former operation, we get the expression of f_Y from f_Z. Conversely, by the multiplication operation, f_Z is generated by

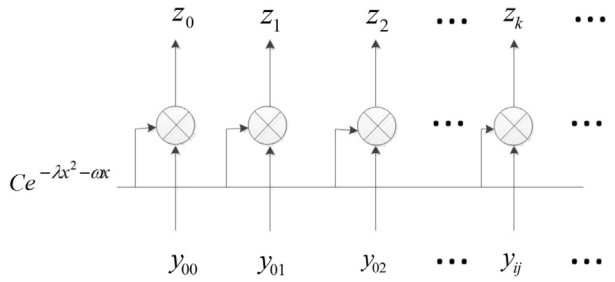

Fig. 2 – Multiplication: each component of f_Y refers to one component of f_Z in multiplication operation, where $k = i \cdot M + j$, M is the number of Gaussian component of f_x.

f_Y that multiplying all the Gaussian components of f_Y by the same multiplier. Fig. 2 illustrates the operation, where all the components of f_Y is multiplied by the same factor "$C\,e^{-\lambda x^2-\omega x}$". Each components of f_Y is transformed into one of f_Z. We call the corresponding two components *component pair* or *pair*. For example, z_0 is the product of y_{00} and the factor, so z_0 and y_{00} are a pair. z_k ($k = i \cdot M + j$) is the product of y_{ij} and the factor, so z_k and y_{ij} are a pair.

Suppose there are two pairs: $y_{i_1 j_1}$ and $z_{i_1 \cdot M + j_1}$, $y_{i_2 j_2}$ and $z_{i_2 \cdot M + j_2}$. Since $y_{i_1 j_1}$ and $y_{i_2 j_2}$ are multiplied by the same factor, if $y_{i_1 j_1}$ and $y_{i_2 j_2}$ are different, $z_{i_1 \cdot M + j_1}$ and $z_{i_2 \cdot M + j_2}$ are different too. So it is a one-to-one mapping between components of f_Z and f_Y. f_Z and f_Y have the same number of components, i.e. $N = M \cdot N$, where the left part of the equation delegates the number of the Gaussian components of f_Z, the right one delegates the number of the Gaussian components of f_Y. This equation holds in two situations:

- $M = 1, N = 1$. Although for any $N > 0$ the equation holds, it is easily checked that all the N components of f_Z have the same σ_Z^2 and μ_Z by the method in Section 5.3. So it is equal to the situation $N = 1$.
- $M > 1, N \to \infty$. Thus when $M > 1$, f_Z is composed of infinite number of Gaussian components.

Consider y_{ij} and z_k which form a component pair, where $k = i \cdot M + j$. From the geometric point of view, z_k stems from y_{ij} by narrowing ($e^{-\lambda x^2}$), translating ($e^{-\omega x}$) and normalizing (C) the curve of y_{ij}. From the algebraic point of view, the three operations are visualized as Eqs. (17)–(19) respectively,

$$e^{-\frac{x^2}{2\left(\sigma_{X_i}^2+\sigma_{Z_j}^2\right)}-\lambda x^2} = e^{-\frac{x^2}{2\sigma_{Z_k}^2}} \tag{17}$$

$$e^{\frac{\left(\mu_{X_i}+\mu_{Z_j}\right)x}{\sigma_{X_i}^2+\sigma_{Z_j}^2}-\omega x} = e^{\frac{\mu_{Z_k} x}{\sigma_{Z_k}^2}} \tag{18}$$

$$C\frac{p_{X_i}p_{Z_j}}{\sqrt{\sigma_{X_i}^2+\sigma_{Z_j}^2}}e^{-\frac{\left(\mu_{X_i}+\mu_{Z_j}\right)^2}{2\left(\sigma_{X_i}^2+\sigma_{Z_j}^2\right)}} = \frac{p_{Z_k}}{\sigma_{Z_k}}e^{-\frac{\mu_{Z_k}^2}{2\sigma_{Z_k}^2}} \tag{19}$$

and the constraints for f_Z are

$$\begin{cases} \sum_j p_{Z_j}\left(\sigma_{Z_j}^2+\mu_{Z_j}^2\right) = \sigma_m^2 & (20) \\ \sum_j p_{Z_j}\mu_{Z_j} = 0 & (21) \\ \sum_j p_{Z_j} = 1. & (22) \end{cases}$$

In these equations $p_{X_i}, \mu_{X_i}, \sigma_{X_i}$ are known, $p_{Z_j}, \mu_{Z_j}, \sigma_{Z_j}$ and λ, ω, C are unknown. Thus the solution is transformed to how to determine the parameters $(p_{Z_j}, \mu_{Z_j}, \sigma_{Z_j}^2)$ of $z_j (j = 0, \ldots, N-1)$ by Eqs. (17)–(19) and constraints (20)–(22). In the following subsections we try to calculate the three parameters of Gaussian components of f_Z when f_x is composed of one, two and more than two Gaussian components.

5.2. f_x with one component

In this situation $M = 1$. f_x is a normal distribution. From Section 4.2 f_Z is a normal distribution too, i.e. $N = 1$, $\sigma_{Z_0}^2 = \sigma_m^2$, $p_{Z_0} = 1$ and $\mu_{Z_0} = 0$. Actually, if we choose $N > 1$, by the method proposed in Section 5.3, we would get $\sigma_{Z_0}^2 = \sigma_{Z_1}^2 = \cdots = \sigma_{Z_{N-1}}^2$ and $\mu_{Z_0} = \mu_{Z_1} = \cdots = \mu_{Z_{N-1}}$, i.e. f_Z is a Gaussian distribution.

5.3. f_x with two components

In this situation $M = 2$, $f_x = (x_0, x_1)$. f_Z has infinite Gaussian components, i.e. $N \to \infty$. In the following we would calculate all the components of f_Z.

5.3.1. Calculate σ_Z^2

For all the component pairs of f_Y and f_Z, the variances are controlled by the same λ. Thus in the same pair the coefficients of "x^2" (the exponent of "e") in Eq. (17) are equal. Suppose $\sigma_{X_0}^2 \geq \sigma_{X_1}^2$, and $\sigma_{Z_0}^2 = \max\{\sigma_{Z_j}^2 \,|\, j \in \mathbb{N}\}$. If $\sigma_{Z_0}^2$ is fixed, all the variances of f_Z and f_Y are determined by the following method.

Step 1 (Fix the first pair). Since $\sigma_{Z_0}^2$ is fixed, we get the variances of two components of f_Y denoted by y_{00} and y_{01} (with variances $\sigma_{Y_{00}}^2 = \sigma_{Z_0}^2 + \sigma_{X_0}^2$ and $\sigma_{Y_{01}}^2 = \sigma_{Z_0}^2 + \sigma_{X_1}^2$) shown in Fig. 3(a). Since $\sigma_{Z_0}^2$ and $\sigma_{X_0}^2$ are all the largest one in the variances of components of f_Z and f_x respectively, $\sigma_{Y_{00}}^2$ is the largest one in all the variances of components of f_Y. y_{00} and z_0 construct a pair, otherwise no y_{ji} pairs z_0.

Step 2 (Fix λ). All the component pairs are generated by the same λ, ω and C, so from any pair the three parameters are fixed. y_{00} and z_0 form a pair, i.e. by narrowing of λ, $\sigma_{Y_{00}}^2$ would become $\sigma_{Z_0}^2$. So we get

$$2\lambda = \frac{1}{\sigma_{Z_0}^2} - \frac{1}{\sigma_{Z_0}^2+\sigma_{X_0}^2} = \frac{\sigma_{X_0}^2}{\sigma_{Z_0}^2\left(\sigma_{Z_0}^2+\sigma_{X_0}^2\right)} > 0. \tag{23}$$

Step 3 (Fix second pair). From $\sigma_{Y_{01}}^2$ and λ, we get $\sigma_{Z_1}^2$ (Eq. (24)) shown in Fig. 3(b). So $\sigma_{Y_{01}}^2$ and $\sigma_{Z_1}^2$ are a pair.

$$
\begin{array}{ll}
\mathrm{Z} & \mathrm{Y} \\
z_0 : \dfrac{1}{\sigma^2_{Z_0}} & y_{00} : \sigma^2_{Y_{00}} = \sigma^2_{Z_0} + \sigma^2_{X_0} \\
 & y_{01} : \sigma^2_{Y_{01}} = \sigma^2_{Z_0} + \sigma^2_{X_1} \\
z_1 : \dfrac{1}{\sigma^2_{Z_1}} = \dfrac{1}{\sigma^2_{y_{01}}} + 2\lambda & y_{10} : \sigma^2_{Y_{10}} = \sigma^2_{Z_1} + \sigma^2_{X_0} \\
 & y_{11} : \sigma^2_{Y_{11}} = \sigma^2_{Z_1} + \sigma^2_{X_1} \\
z_2 : \dfrac{1}{\sigma^2_{Z_2}} = \dfrac{1}{\sigma^2_{y_{10}}} + 2\lambda & y_{20} : \sigma^2_{Y_{20}} = \sigma^2_{Z_2} + \sigma^2_{X_0} \\
 & y_{21} : \sigma^2_{Y_{21}} = \sigma^2_{Z_2} + \sigma^2_{X_1} \\
\cdots & \cdots \\
z_{2j} : \dfrac{1}{\sigma^2_{Z_{2j}}} = \dfrac{1}{\sigma^2_{y_{j0}}} + 2\lambda & y_{(2j)0} : \sigma^2_{Y_{(2j)0}} = \sigma^2_{Z_{2j}} + \sigma^2_{X_0} \\
 & y_{(2j)1} : \sigma^2_{Y_{(2j)1}} = \sigma^2_{Z_{2j}} + \sigma^2_{X_1} \\
z_{2j+1} : \dfrac{1}{\sigma^2_{Z_{2j+1}}} = \dfrac{1}{\sigma^2_{y_{j1}}} + 2\lambda & y_{(2j+1)0} : \sigma^2_{Y_{(2j+1)0}} = \sigma^2_{Z_{2j+1}} + \sigma^2_{X_0} \\
 & y_{(2j+1)1} : \sigma^2_{Y_{(2j+1)1}} = \sigma^2_{Z_{2j+1}} + \sigma^2_{X_1}
\end{array}
\tag{24}
$$

Step 4 (Fix other pairs). When $\sigma^2_{Z_1}$ is fixed, combing λ, the other two σ^2_Y (denoted by $\sigma^2_{Y_{10}}$ and $\sigma^2_{Y_{11}}$) are fixed (Fig. 3(c)). Then the corresponding pair members $\sigma^2_{Z_2}$ and $\sigma^2_{Z_3}$ can be calculated (Fig. 3(d))···. In this way we can get the pairs (z_{2j+i}, y_{ji}), $j = 0, 1, 2, \ldots$ and $i = 0, 1$, and the variances (Fig. 3(e)). Eq. (24) shows the process of calculating all the variances. Thus given $\sigma^2_{Z_0}$, all the $\sigma^2_{Z_j}$ are fixed.

We represent $\sigma^2_{Z_j}$ with one general term formula. Suppose the binary form of j is (j_0, j_1, …, j_t), $\sigma^2_{Z_j}$ has the general term formula as

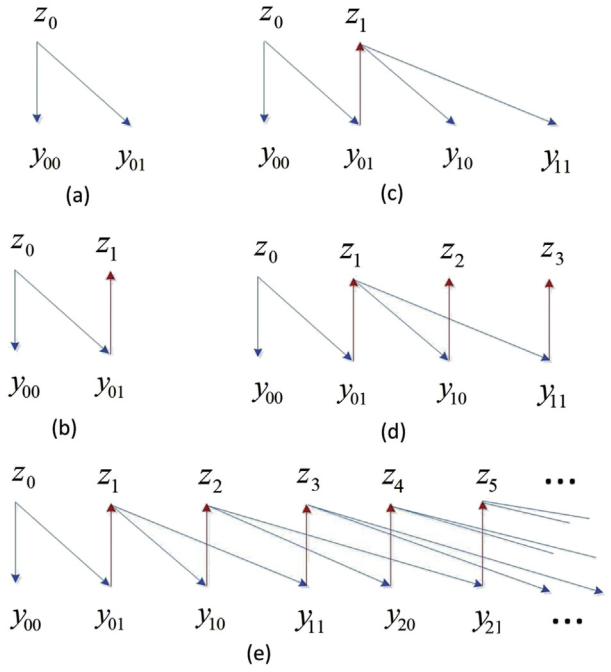

Fig. 3 – The generation of all σ^2_Z and σ^2_Y. The arrows show the generating order of components of f_Z and f_Y. The two components in the same vertical line compose a pair.

$$
\sigma^2_{Z_{(j_0 j_1 \ldots j_t)}} = \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_{j_t}} + \sigma^2_{Z_{(j_0 j_1 \ldots j_{t-1})}}}} \tag{25}
$$

5.3.2. *Calculate* μ_Z

In the above we fix the coefficients of "x^2" of Eq. (17) and find out the component pairs ($z_{2\cdot j+i}$, y_{ji}), $j = 0, 1, 2, \ldots$ and $i = 0, 1$. The method of calculating μ_Z is the same as the method of generating σ^2_Z. Based on Eq. (18) we can fix the coefficients of "x". Since (z_0, y_{00}) is a pair,

$$
\omega = \frac{\mu_{Z_0} + \mu_{X_0}}{\sigma^2_{Z_0} + \sigma^2_{X_0}} - \frac{\mu_{Z_0}}{\sigma^2_{Z_0}}. \tag{26}
$$

Then μ_{Z_1} is fixed by $\mu_{Y_{01}}$ and ω (all the components of f_Y translate the same distance under the normalized variances). From μ_{Z_1} two expectations of f_Y, $\mu_{Y_{10}}$ and $\mu_{Y_{11}}$, are generated. Then μ_{Z_2} and μ_{Z_3} are fixed···. By the iterative method, if μ_{Z_0} is fixed, all the μ_{Z_j} are fixed. Eq. (27) shows the calculation process.

$$
\begin{array}{ll}
\mathrm{Z} & \mathrm{Y} \\
z_0 : \dfrac{\mu_{Z_0}}{\sigma^2_{Z_0}} & y_{00} : \mu_{Y_{00}} = \mu_{Z_0} + \mu_{X_0} \\
 & y_{01} : \mu_{Y_{01}} = \mu_{Z_0} + \mu_{X_1} \\
z_1 : \dfrac{\mu_{Z_1}}{\sigma^2_{Z_1}} = \dfrac{\mu_{Y_{01}}}{\sigma^2_{Z_0} + \sigma^2_{X_1}} - \omega & y_{10} : \mu_{Y_{10}} = \mu_{Z_1} + \mu_{X_0} \\
 & y_{11} : \mu_{Y_{11}} = \mu_{Z_1} + \mu_{X_1} \\
z_2 : \dfrac{\mu_{Z_2}}{\sigma^2_{Z_2}} = \dfrac{\mu_{Y_{10}}}{\sigma^2_{Z_1} + \sigma^2_{X_0}} - \omega & y_{20} : \mu_{Y_{20}} = \mu_{Z_2} + \mu_{X_0} \\
 & y_{21} : \mu_{Y_{21}} = \mu_{Z_2} + \mu_{X_1} \\
\cdots & \cdots \\
z_{2j} : \dfrac{\mu_{Z_{2j}}}{\sigma^2_{Z_{2j}}} = \dfrac{\mu_{Y_{j0}}}{\sigma^2_{Z_j} + \sigma^2_{X_0}} - \omega & y_{(2j)0} : \mu_{Y_{(2j)0}} = \mu_{Z_{2j}} + \mu_{X_0} \\
 & y_{(2j)1} : \mu_{Y_{(2j)0}} = \mu_{Z_{2j}} + \mu_{X_1} \\
z_{2j+1} : \dfrac{\mu_{Z_{2j+1}}}{\sigma^2_{Z_{2j+1}}} = \dfrac{\mu_{Y_{j1}}}{\sigma^2_{Z_j} + \sigma^2_{X_1}} - \omega & y_{(2j+1)0} : \mu_{Y_{(2j+1)0}} = \mu_{Z_{2j+1}} + \mu_{X_0} \\
 & y_{(2j+1)1} : \mu_{Y_{(2j+1)0}} = \mu_{Z_{2j+1}} + \mu_{X_1}
\end{array}
\tag{27}
$$

Suppose the binary form of j is (j_0, j_1, …, j_t), μ_{Z_j} has the general term formula as

$$
\mu_{Z_{(j_0 j_1 \ldots j_t)}} = \sigma^2_{Z_{(j_0 j_1 \ldots j_t)}} \cdot \left(\frac{\mu_{Z_{(j_0 j_1 \ldots j_{t-1})}} + \mu_{X_{j_t}}}{\sigma^2_{Z_{(j_0 j_1 \ldots j_{t-1})}} + \sigma_{X^2_{j_t}}} - \omega \right). \tag{28}
$$

5.3.3. *Calculate* p_Z

The method of calculating p_Z is the same as the method of generating σ^2_Z too. From Eq. (19) the constant term of each pair have the same ratio C. Since (z_0, y_{00}) is a pair, if p_{Z_0} is fixed,

$$
C = \frac{1}{p_{X_0}} \sqrt{1 + \frac{\sigma^2_{X_0}}{\sigma^2_{Z_0}}}\, e^{\frac{\mu^2_{X_0}\sigma^2_{Z_0} + \mu^2_{Z_0}\sigma^2_{X_0} + 2\mu_{X_0}\mu_{Z_0}\sigma^2_{Z_0}}{2\sigma^2_{Z_0}\left(\sigma^2_{X_0} + \sigma^2_{Z_0}\right)}}. \tag{29}
$$

Then p_{Z_1} is fixed by $p_{Y_{01}}$ and C (all the components of f_Y are normalized with the same C). From p_{Z_1} two coefficients of f_Y, $p_{Y_{10}}$ and $p_{Y_{11}}$, are generated. Then p_{Z_2} and p_{Z_3} are fixed···. By the iterative method, if p_{Z_0} is fixed, all the p_{Z_j} are fixed. Eq. (30) shows the calculation process.

$$
\begin{array}{ll}
Z & Y \\
z_0 : p_{Z_0} & y_{00} : p_{Y_{00}} = p_{Z_0} p_{X_0} \\
 & y_{01} : p_{Y_{01}} = p_{Z_0} p_{X_1} \\
z_1 : p_{Z_1} = C p_{Y_{01}} \sqrt{\frac{\sigma_{Z_1}^2}{\sigma_{Z_0}^2 + \sigma_{X_1}^2}} e^{\frac{\mu_{Z_1}^2}{2\sigma_{Z_1}^2} - \frac{\left(\mu_{X_1} + \mu_{Z_0}\right)^2}{2\left(\sigma_{X_1}^2 + \sigma_{Z_0}^2\right)}} & y_{10} : p_{Y_{10}} = p_{Z_1} p_{X_0} \\
 & y_{11} : p_{Y_{11}} = p_{Z_1} p_{X_1} \\
z_2 : p_{Z_2} = C p_{Y_{10}} \sqrt{\frac{\sigma_{Z_2}^2}{\sigma_{Z_1}^2 + \sigma_{X_0}^2}} e^{\frac{\mu_{Z_2}^2}{2\sigma_{Z_2}^2} - \frac{\left(\mu_{X_0} + \mu_{Z_1}\right)^2}{2\left(\sigma_{X_0}^2 + \sigma_{Z_1}^2\right)}} & y_{20} : p_{Y_{20}} = p_{Z_2} p_{X_0} \\
 & y_{21} : p_{Y_{21}} = p_{Z_2} p_{X_1} \\
\cdots & \cdots \\
z_{2j} : p_{Z_{2j}} = C p_{Y_{j0}} \sqrt{\frac{\sigma_{Z_{2j}}^2}{\sigma_{Z_j}^2 + \sigma_{X_0}^2}} e^{\frac{\mu_{Z_{2j}}^2}{2\sigma_{Z_{2j}}^2} - \frac{\left(\mu_{X_0} + \mu_{Z_j}\right)^2}{2\left(\sigma_{X_0}^2 + \sigma_{Z_j}^2\right)}} & y_{(2j)0} : p_{Y_{(2j)0}} = p_{Z_{2j}} p_{X_0} \\
 & y_{(2j)1} : p_{Y_{(2j)0}} = p_{Z_{2j}} p_{X_1} \\
z_{2j+1} : p_{Z_{2j+1}} = C p_{Y_{j1}} \sqrt{\frac{\sigma_{Z_{2j+1}}^2}{\sigma_{Z_j}^2 + \sigma_{X_1}^2}} e^{\frac{\mu_{Z_{2j+1}}^2}{2\sigma_{Z_{2j+1}}^2} - \frac{\left(\mu_{X_1} + \mu_{Z_j}\right)^2}{2\left(\sigma_{X_1}^2 + \sigma_{Z_j}^2\right)}} & y_{(2j+1)0} : p_{Y_{(2j+1)0}} = p_{Z_{2j+1}} p_{X_0} \\
 & y_{(2j+1)1} : p_{Y_{(2j+1)0}} = p_{Z_{2j+1}} p_{X_1}
\end{array}
\tag{30}
$$

Suppose the binary form of j is $(j_0, j_1, \ldots, j_t)$, p_{Z_j} has the general term formula as

$$
p_{Z_{(j_0 j_1 \ldots j_t)}} = C\sigma_{Z_{(j_0 j_1 \ldots j_t)}} \cdot \frac{p_{Z_{(j_0 j_1 \ldots j_{t-1})}} p_{X_{j_t}}}{\sqrt{\sigma_{Z_{(j_0 j_1 \ldots j_{t-1})}}^2 + \sigma_{X_{j_t}}^2}} \cdot e^{\frac{\mu_{Z_{(j_0 j_1 \ldots j_t)}}^2}{2\sigma_{Z_{(j_0 j_1 \ldots j_t)}}^2} - \frac{\left(\mu_{X_{j_t}} + \mu_{Z_{(j_0 j_1 \ldots j_{t-1})}}\right)^2}{2\left(\sigma_{X_{j_t}}^2 + \sigma_{Z_{(j_0 j_1 \ldots j_{t-1})}}^2\right)}}. \tag{31}
$$

Now for constructing f_Z, the unknown numbers of Eq. (9) only are $\sigma_{Z_0}^2, \mu_{Z_0}$ and p_{Z_0}, which are determined by constraints Eqs. (20)–(22).

5.4. f_x with multiple components

When f_x is composed of more than two Gaussian components ($M > 2$), the calculation process is similar as the situation $M = 2$. f_Z consists of infinite number of Gaussian components ($N \to \infty$). Given one Gaussian component with the largest variance, other components are calculated. A one to one mapping between the components of f_Z and f_Y is constructed, i.e. y_{ji} and $z_{M \cdot j+i}$ are a pair, where $i = 0, 1, \ldots, M-1$ and $j = 0, 1, \ldots$. Suppose the base-M form of j is $(j_0, j_1, \ldots, j_t)$, $\sigma_{Z_j}^2$, μ_{Z_j} and p_{Z_j} have the general term formula Eqs. (25), (28), and (31) respectively. The formats are the same as the situation $M = 2$, but here $t \in \{0, 1, \ldots, M-1\}$. Furthermore, the equations fixing $\sigma_{Z_0}^2, \mu_{Z_0}$ and p_{Z_0} are the same as Eqs. (20)–(22).

From above analysis, if one Gaussian component of f_Z which has the largest variance among all the components of f_Z is fixed, all other components of f_Z can be calculated by Eqs. (25), (28), and (31). Theoretically speaking, we greatly reduce the number of unknown numbers in constructing f_Z by Eq. (9) from infinite ones to only three ones ($\sigma_{Z_0}^2$, μ_{Z_0} and p_{Z_0}). Moreover, we give the three Eqs. (20)–(22), which are the constraints of the three parameters.

6. Properties of Gaussian components

Based on the investigation in the above section, we only need to calculate the three parameters $\sigma_{Z_0}^2$, μ_{Z_0} and p_{Z_0}. However, it is impossible to calculate infinite number of Gaussian components of f_Z. In this section we explore the properties of these components, by which f_Z could be approximated by finite number of Gaussian components with high accuracy. We mainly consider the properties of $M = 2$. The situation $M > 2$ is similar, which can be divided into $M - 1$ independent situations.

By the generation order of Gaussian components, we construct a tree of the components of f_Z illustrated in Fig. 4, which is another form of Fig. 3 ignoring the components of f_Y. It is composed of the root z_0 and its right subtree, where the left child is generated by the parent and x_0, and the right child is generated by the parent and x_1, where $\sigma_{X_0}^2 \geq \sigma_{X_1}^2$. Specifically, the tree also delegate the generation order of σ_Z^2, μ_Z and p_Z. Based on the tree, in the following we investigate the properties of the three parameters respectively.

6.1. Properties of variance parameter

In this subsection we focus on the variances of all the components. From this binary tree (Fig. 4), where z_0 has the largest variance $\sigma_{Z_0}^2$, we have the following properties.

Lemma 1. *For any $j \not\equiv N$, $\sigma_{Z_{2j}}^2 \geq \sigma_{Z_{2j+1}}^2$.*

The proof is given in Appendix B.

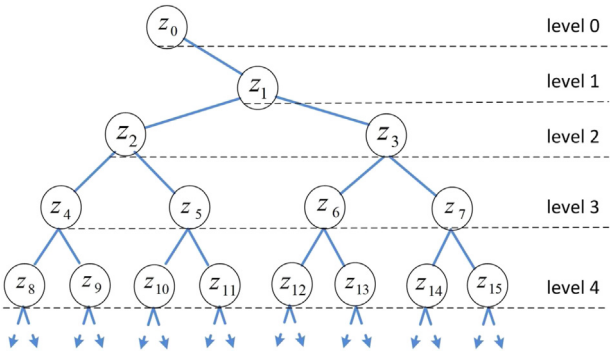

Fig. 4 – Binary tree of Gaussian components of f_Z.

From this lemma, the left child is larger than or equal to the right child.

Lemma 2. *For any $j \notin \mathbb{N}$, $\sigma^2_{Z_{2j}} \geq \sigma^2_{Z_j}$.*

The proof is given in Appendix C.

From this lemma, the left child is larger than or equal to the parent. Consider the condition of equation holds, if $\sigma^2_{Z_j} = \sigma^2_{Z_0}$ for any j, $\sigma^2_{X_0} = \sigma^2_{X_1}$. Thus the equation of Lemma 2 holds under the condition $\sigma^2_{X_0} = \sigma^2_{X_1}$ too.

Theorem 3. *For any $j \notin \mathbb{N}$,*

$$s_\infty \leq \sigma^2_{Z_j} \leq \sigma^2_{Z_0},$$

where $s_\infty = \sqrt{\lambda^2\sigma^4_{X_1} + 2\lambda\sigma^2_{X_1}} - \lambda\sigma^2_{X_1}/2\lambda$.

The proof is given in Appendix D.

This theorem shows the range of σ^2_Z. Suppose $\sigma^2_{Z_0}/\sigma^2_{X_0} = t_0$, $\sigma^2_{X_1}/\sigma^2_{X_0} = t_1$, where $t_1 \leq 1$. The ratio of maximum of the interval to minimum is

$$\frac{\sigma^2_{Z_0}}{s_\infty} = \frac{\sqrt{t_1^2 + 4t_0(t_0+1)t_1} + t_1}{2(t_0+1)t_1}. \tag{32}$$

Shown in Fig. 5, when $\sigma^2_{X_0}$ is not much larger than $\sigma^2_{X_1}$, the interval is small (Z-axis delegates the ratio of maximum of the interval to minimum). When $t_1 \to 1$, $\sigma^2_{Z_0}/s_\infty \to 1$, which means when f_x is composed of two Gaussian components with almost the same variance, variances of all components of f_Z are almost equal.

Lemma 3. *For any $j \notin \mathbb{N}$, $\sigma^2_{Z_j} \geq \sigma^2_{Z_{2j+1}}$.*

The proof is given in Appendix E.

From this lemma, the parent is larger than or equal to the right child.

When $\sigma^2_{Z_j} = s_\infty$, we have $\sigma^2_{Z_0} = \sigma^2_{Z_1} = \cdots = s_\infty$. From Theorem 3, $\sigma^2_{X_0} = \sigma^2_{X_1}$. Thus the equality in this lemma holds as the same as the above lemmas.

Lemma 4. *For any $j \in [2^t, 2^{t+1})$, $t > 0$ If j is even, $\sigma^2_{Z_{2t}} \geq \sigma^2_{Z_j} \geq \sigma^2_{Z_{2^{t+1}-2}}$. If j is odd, $\sigma^2_{Z_{2^t+1}} \geq \sigma^2_{Z_j} \geq \sigma^2_{Z_{2^{t+1}-1}}$.*

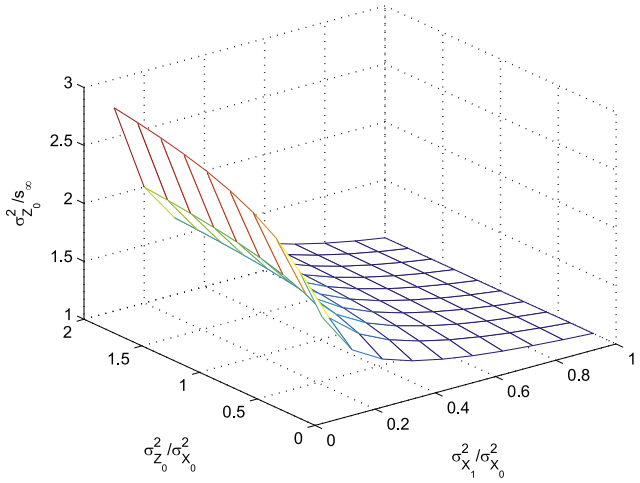

Fig. 5 – The influence of $\sigma^2_{X_1}/\sigma^2_{X_0}$ and $\sigma^2_{Z_0}/\sigma^2_{X_0}$ to $\sigma^2_{Z_0}/s_\infty$, which is the ratio of maximum of the interval of variance $\sigma^2_{Z_j}$ to minimum.

The proof is given in Appendix F.

From this lemma, both for variances with odd indices and for variances with even indices, in the same level the largest variance is the leftmost one, the smallest variance is the rightmost one.

Lemma 5. *For any $j \notin N^+$, if j is even, $\sigma^2_{Z_0} \geq \sigma^2_{Z_j} \geq 1/2\lambda + 1/\sigma^2_{X_0} + s_\infty$. If j is odd, $\sigma^2_{Z_1} \geq \sigma^2_{Z_j} \geq s_\infty$.*

The proof is given in Appendix G.

This lemma shows the ranges of variances with odd indices and even indices respectively. Suppose $\sigma^2_{Z_0}/\sigma^2_{X_0} = t_0$, $\sigma^2_{X_1}/\sigma^2_{X_0} = t_1 \leq 1$ as before. We have the following theorem.

Theorem 4. *All the σ^2_Z with even orders and odd orders are located in $[1/2\lambda + 1/\sigma^2_{X_0} + s_\infty, \sigma^2_{Z_0}]$ and $[s_\infty, \sigma^2_{Z_1}]$ respectively. If $t_1 \to 1$, the length of the two intervals converge to 0.*

The proof is given in Appendix H.

This property is more precise than Theorem 3 (shown in Figs. 6 and 7). For example, under the condition that $t_0 = 0.8$, if $t_1 = 0.5$, all the σ^2_Z lie in [59.60, 74.76]. All the σ^2_Z with odd indices and even indices lie in [59.60, 63.82] and [71.84, 74.76] respectively. If $t_1 = 0.8$, all the σ^2_Z lie in [70.31, 75.34]. All the σ^2_Z with odd indices and even indices lie in [70.31, 71.39] and [74.39, 75.34] respectively. Thus from this theorem, when $\sigma^2_{X_0}$ is not much larger than $\sigma^2_{X_1}$, all the variances can be replaced by two variances $\sigma^2_{Z_0}$ (even indices) and $\sigma^2_{Z_1}$ (odd indices).

For $M > 2$, all the properties are similar to the situation $M = 2$. The binary tree is extended to an M-branches tree, which also can be regarded as the mixture of $M - 1$ binary trees ($\sigma^2_{X_0}$ and $\sigma^2_{X_1}$, $\sigma^2_{X_0}$ and $\sigma^2_{X_2}$, …, $\sigma^2_{X_0}$ and $\sigma^2_{X_{M-1}}$). The properties of the tree are the similar too. All the variances are divided into M sets, each of which has a small range.

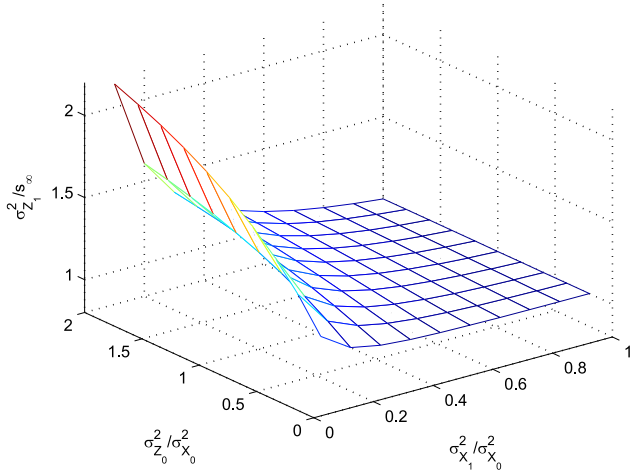

Fig. 6 – The influence of $\sigma^2_{X_1}/\sigma^2_{X_0}$ and $\sigma^2_{Z_0}/\sigma^2_{X_0}$ to $\sigma^2_{Z_1}/s_\infty$, which is the ratio of maximum of the interval of the variance $\sigma^2_{Z_j}$ with odd indices to minimum.

6.2. *Properties of expectation parameter*

Consider the situation that $\sigma^2_{X_1}$ is not much smaller than $\sigma^2_{X_0}$ (e.g. $t_1 \geq 0.5$), where all the components with odd indices have the variance $\sigma^2_{Z_1}$ and components with even indices have the variance $\sigma^2_{Z_0}$, i.e. for $j \in \mathbb{N}$, $\sigma^2_{Z_{2j}} = \sigma^2_{Z_0}$ and $\sigma^2_{Z_{2j+1}} = \sigma^2_{Z_1}$. Based on this approximation of σ^2_Z, we investigate the properties of the expectations of components. The general term formula of μ_Z Eq. (28) can be refined as

$$\mu_{Z_{4j}} = \sigma^2_{Z_{4j}}\left(\frac{\mu_{Z_{2j}} + \mu_{X_0}}{\sigma^2_{Z_{2j}} + \sigma^2_{X_0}} - \omega\right) = h_0\mu_{Z_{2j}} + H_0 \tag{33}$$

$$\mu_{Z_{4j+1}} = \sigma^2_{Z_{4j+1}}\left(\frac{\mu_{Z_{2j}} + \mu_{X_1}}{\sigma^2_{Z_{2j}} + \sigma^2_{X_1}} - \omega\right) = h_1\mu_{Z_{2j}} + H_1 \tag{34}$$

$$\mu_{Z_{4j+2}} = \sigma^2_{Z_{4j+2}}\left(\frac{\mu_{Z_{2j+1}} + \mu_{X_0}}{\sigma^2_{Z_{2j+1}} + \sigma^2_{X_0}} - \omega\right) = h_2\mu_{Z_{2j+1}} + H_2 \tag{35}$$

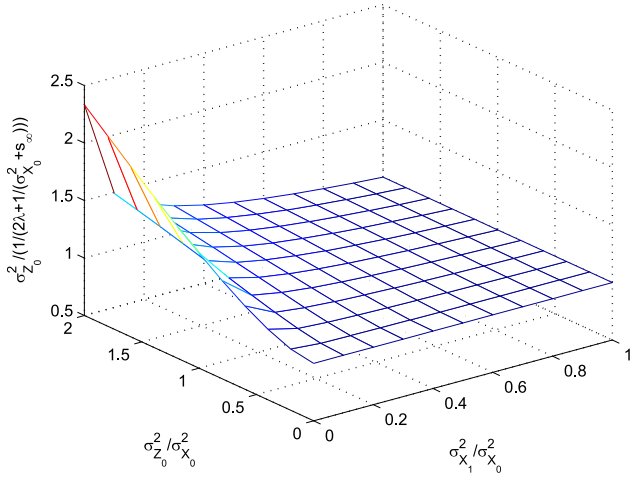

Fig. 7 – The influence of $\sigma^2_{X_1}/\sigma^2_{X_0}$ and $\sigma^2_{Z_0}/\sigma^2_{X_0}$ to $\sigma^2_{Z_0}/(1/2\lambda + 1/\sigma^2_{X_0} + s_\infty)$, which is the ratio of maximum of the interval of the variance $\sigma^2_{Z_j}$ with even indices to minimum.

$$\mu_{Z_{4j+3}} = \sigma^2_{Z_{4j+3}}\left(\frac{\mu_{Z_{2j+1}} + \mu_{X_1}}{\sigma^2_{Z_{2j+1}} + \sigma^2_{X_1}} - \omega\right) = h_3\mu_{Z_{2j+1}} + H_3, \tag{36}$$

where

$$h_0 = \frac{t_0}{t_0 + 1}, \quad H_0 = (1 - h_0)\mu_{Z_0},$$

$$h_1 = \frac{t_0(t_0 + 1)}{t_0^2 + 2t_0 + t_1},$$

$$H_1 = (1 - h_1)\mu_{Z_0} - t_0(1 - h_1)\mu_{X_0} + h_1\mu_{X_1},$$

$$h_2 = \frac{t_0(t_0^2 + 2t_0 + t_1)}{t_0^3 + (t_1 + 2)t_0^2 + (t_1 + 2)t_0 + t_1},$$

$$H_2 = (1 - h_0)\mu_{Z_0} - t_0(1 - h_0)\mu_{X_0} + h_2\mu_{X_0},$$

$$h_3 = \frac{t_0(t_0 + 1)(t_0 + t_1)}{t_0^3 + (2t_1 + 1)t_0^2 + 3t_1t_0 + t_1^2},$$

$$H_3 = (1 - h_1)\mu_{Z_0} - t_0(1 - h_1)\mu_{X_0} + h_3\mu_{X_1}.$$

Consider the tree in Fig. 4, suppose l is the l-th level of the tree from the root. z_0 is at the 0-th level. $z_{2^{l-1}}, z_{2^{l-1}+1}, \ldots, z_{2^l-1}$ are at the l-th level. We have the following properties.

Lemma 6. *When the level $l \to \infty$,*

$$\mu_{Z_{2^l}} = \mu_{Z_{2^{l+1}}} = \mu_{Z_0}, \tag{37}$$

$$\mu_{Z_{2^{l+1}-1}} = \mu_{Z_{2^{l+2}-1}} = \mu_\infty, \tag{38}$$

where μ_∞=$H_3/1-h_3$.

The proof is given in Appendix I.

This lemma shows that with the increase of level of the tree, the leftmost μ_Z converge to μ_{Z_0}, and the rightmost μ_Z converge to μ_∞.

Lemma 7. *When the level $l \to \infty$, the μ_Z at level l are not related to the root of the tree. Approximately, when t_0 is close to 0, a small l can be chosen.*

The proof is given in Appendix J.

From Eqs. (33)–(36), when t_1 is close to 1, we have the approximate relationship $h_0 = h_1 = h_2 = h_3$. When t_1 is fixed, h_i are the increasing functions of t_0. Figs. 8 and 9 illustrate the relationship.

Theorem 5. *μ_Z can be regarded as a periodic sequence with the period 2^l, where l is large enough.*

The proof is given in Appendix K.

This theorem shows the sequence of μ_Z can be regarded as a periodic sequence with 2^l. The larger l is, the more accurate the approximation is. From Lemma 7 l is determined by t_0. When t_0 is small, a small l can be chosen.

6.3. Properties of weight parameter

6.3.1. General properties

Suppose 2^l is the period of μ_Z. Consider the two sequences

$$\left\{p_{Z_0}, p_{Z_1}, \ldots, p_{Z_{2^{l'+1}-1}}\right\}$$

and

$$\left\{p_{Z_{2^{l'}+1}}, p_{Z_{2^{l'}+1+1}}, \ldots, p_{Z_{2^{l'+2}-1}}\right\},$$

where $l' \geq l$. Refer to Fig. 4, the former sequence contains all the p_Z at first $l' + 1$ levels (p_{Z_0} is at level 0). The latter one contains all the p_Z at level $l' + 2$. Obviously the number of elements is the same. We have the following theorem for p_Z:

Theorem 6. *Consider the two sequences above, the ratio of the two elements with the same order is equal to the ratio of their parents, i.e.*

$$\frac{p_{Z_{2^{l'+1}+2k}}}{p_{Z_{2k}}} = \frac{p_{Z_{2^{l'+1}+2k+1}}}{p_{Z_{2k+1}}} = \frac{p_{Z_{2^{l'}+k}}}{p_{Z_k}} \tag{39}$$

The proof is given in Appendix L.

From Theorem 6 the process can be iterated until all the parent nodes are located at the first l levels. So the infinite number of p_Z can be replaced by the combination of the first 2^{l+1} p_Z.

Along the order of p_Z, the sequence p_Z is divided into multiple subsequences, denoted by S_0, S_1, … , each of which contains 2^l elements. Define $S_b = R_{ab}{}^*S_a$, where R_{ab} is a sequence containing 2^l elements, "*" is the operation that the i-th elements of R_{ab} and S_a multiply each other. For example, $S_0 = R_{00}{}^*S_0$, where $R_{00} = [1, 1, \ldots, 1]$. If all the elements of R_{ab} are equal to r_{ab}, we simplify $S_b = R_{ab}{}^*S_a$ as $S_b = r_{ab}S_a$ or $S_a = S_b/r_{ab}$. Fig. 10 shows an example of dividing p_Z, where the period of μ_Z is 2^1. Thus each subsequence contains 2 elements. Suppose $p_{Z_{2^l+i}}/p_{Z_i} = r_i$, $i = 0, 1, \ldots, 2^l - 1$. The elements of R_{ab} are relevant to $\{r_i | i = 0, 1, \ldots, 2^l - 1\}$. From theorem 6 all the subsequences can be calculated, where the process is shown in Eq. (40).

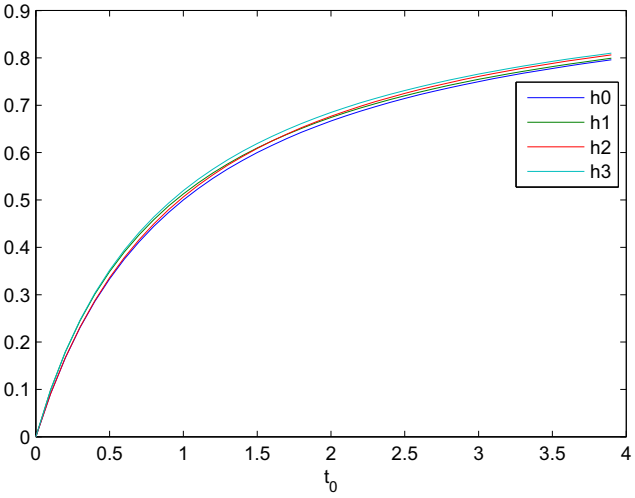

Fig. 8 – The relationship between h_i and t_0, where $t_1 = 0.9$.

Given p_{Z_0}, the other p_{Z_j} are fixed. If we choose two different p_{Z_0} denoted by $p_{Z_{0a}}$ and $p_{Z_{0b}}$ respectively, from Eq. (31) the corresponding j-th p_Z $p_{Z_{ja}}$ and $p_{Z_{jb}}$ have the relationship as $p_{Z_{jb}}/p_{Z_{ja}} = p_{Z_{0a}}/p_{Z_{0b}}$. Thus the p_{Z_0} can be calculated as following: at first p_{Z_0} is initialized with arbitrary non-zero value (e.g. $p_{Z_0} = 1$), and all the other p_{Z_j} are fixed by Eq. (31). Then by constraint Eq. (22), all the p_Z are normalized by dividing the sum of p_Z, i.e.

$$p_{Z_j} = \frac{1}{\sum_{i=0}^{\infty} p_{Z_{ja}}} p_{Z_{ja}}. \tag{41}$$

6.3.2. Special property

Here we focus on a special situation that the period of μ_Z is 2, where $\mu_{Z_0} = \mu_{Z_2} = \cdots$ and $\mu_{Z_1} = \mu_{Z_3} = \cdots$. Under this constraint, we have either of the following results:

$$\begin{array}{lll}
\text{level} & & \\
0\tilde{}l: & S_0 & = [1, 1, 1, \cdots, 1]{}^*S_0 \\
l+1: & S_1 & = [r_0, r_1, r_2, \cdots, r_{2^l-1}]{}^*S_0 \\
l+2: & S_2 & = [r_0, r_0, r_1, \cdots, r_{2^{l-1}-1}]{}^*S_0 \\
 & S_{2+1} & = [r_{2^{l-1}}, r_{2^{l-1}}, r_{2^{l-1}+1}, \cdots, r_{2^l-1}]{}^*S_1 \\
l+3: & S_{2^2} & = [r_0, r_0, r_0, \cdots, r_{2^{l-2}-1}]{}^*S_0 \\
 & S_{2^2+1} & = [r_{2^{l-2}}, r_{2^{l-2}}, r_{2^{l-2}}, \cdots, r_{2^{l-1}-1}]{}^*S_1 \\
 & S_{2^2+2} & = [r_{2^{l-1}}, r_{2^{l-1}}, r_{2^{l-1}}, \cdots, r_{2^{l-1}+2^{l-2}-1}]{}^*S_2 \\
 & S_{2^2+3} & = [r_{2^{l-1}+2^{l-2}}, r_{2^{l-1}+2^{l-2}}, r_{2^{l-1}+2^{l-2}}, \cdots, r_{2^l-1}]{}^*S_3 \\
\cdots & \cdots & \\
l+k: & \cdots & \\
 & S_{2^{k-1}+i} & = \left[r_{\lfloor i\cdot 2^{l-k+1}\rfloor}, \cdots, r_{\lfloor i\cdot 2^{l-k+1}\rfloor + \left\lfloor \frac{j}{2^{k-1}} \right\rfloor}, \cdots, r_{\lfloor i\cdot 2^{l-k+1}\rfloor + \left\lfloor \frac{2^l-1}{2^{k-1}} \right\rfloor}\right]{}^*S_i \\
\cdots & \cdots &
\end{array} \tag{40}$$

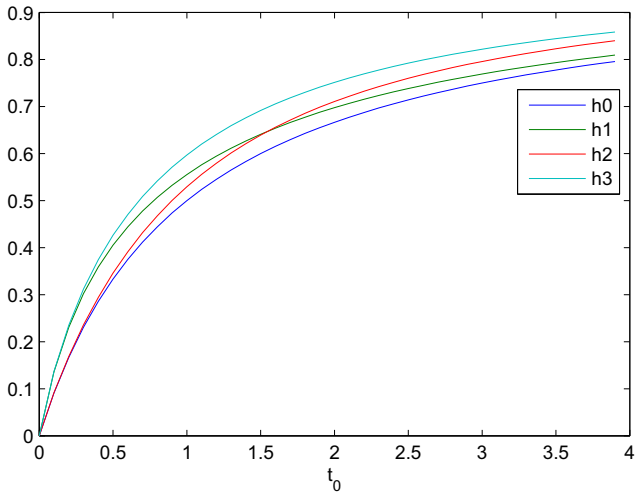

Fig. 9 – The relationship between h_i and t_0, where $t_1 = 0.6$.

1. $t_1 \to 1, t_0 \to 0$,
2. $t_1 \to 1, |\mu_{X_1} - \mu_{X_0}| \to 0$.

In this situation, we have the following theorem.

Theorem 7. *If the period of μ_Z is 2,*

$$r_0 = r_1. \tag{42}$$

The proof is given in Appendix M.

From this theorem, when the period of μ_Z is 2, the complexity of the optimization problem can be reduced greatly.

7. Approximation of optimal distribution

In this section we consider how to approximate f_Z by finite Gaussian components. The approximate distribution is denoted by f_{Zap}. From the properties of the Gaussian components in the above section, f_{Zap} can be split into 2^l weighted Gaussian functions. In the following at first we consider the general situation, and propose an algorithm for expressing f_{Zap}. Then we investigate two special cases. The first is the period of μ_Z is 2, where f_{Zap} contains two Gaussian components. The second is $|\mu_{X_0} - \mu_{X_1}| \gg 0$, where the two components are far away from each other.

7.1. General expression

Suppose f_{Zap} contains 2^l weighted Gaussian functions, the weight sequence is expressed by S, denoted by

$$S = \mathop{\cup}_{i=0}^{\infty} S_i = \sum_{i=0}^{\infty} R_{0i} * WS_0. \tag{43}$$

Then by normalization, S is fixed. According to Eq. (40) R_{0i} can be calculated. Since the optimal f_Z exists, when i is large enough, the normalized S would be stable, the elements of which are the Gaussian components of the optimal f_Z.

Consider the constraints (20) and (21), which can be expressed by the functions of $\sigma_{Z_0}^2$ and μ_{Z_0}, i.e.

$$f_1\left(\sigma_{Z_0}^2, \mu_{Z_0}\right) = \sum_{i=0}^{2^l-1} cp_{Z_i}\left(\sigma_{Z_i}^2 + \mu_{Z_i}^2\right) \tag{44}$$

$$f_2\left(\mu_{Z_0}\right) = \sum_{i=0}^{2^l-1} cp_{Z_i}\mu_{Z_i}, \tag{45}$$

where $f_2(\mu_{Z_0}) = 0$ and $f_1(\sigma_{Z_0}^2, \mu_{Z_0}) = \sigma_m^2$.

From Fig. 11 shows the relationship between μ_{Z_0} and f_2. $f_2(\mu_{Z_0})$ is a monotone increasing functions of μ_{Z_0}. Similarly, shown in Fig. 12 when μ_0 is fixed, f_1 is a monotone increasing functions of $\sigma_{Z_0}^2$. Thus μ_{Z_0} and $\sigma_{Z_0}^2$ can be calculated by Newton iteration method.

Based on the analysis above, we propose **Algorithm 1** to calculate the Gaussian components of f_{Zap} based on the accuracy requirement bound σ_m^2. In the algorithm f_{Zap} consists of 2^l Gaussian components, L is chosen to satisfy $L > l$ so that S is stable. "maxNumber" and "minNumber" are two constants which are large and small enough respectively. At line 20 the function "sum()" calculate the summation of the elements in the sequence. If l and L are infinite, f_{Zap} becomes f_Z.

The complexity of the algorithm is $O(2^L)$, where $L > l$. When l is large, it is hard to calculate the accurate S. In the next

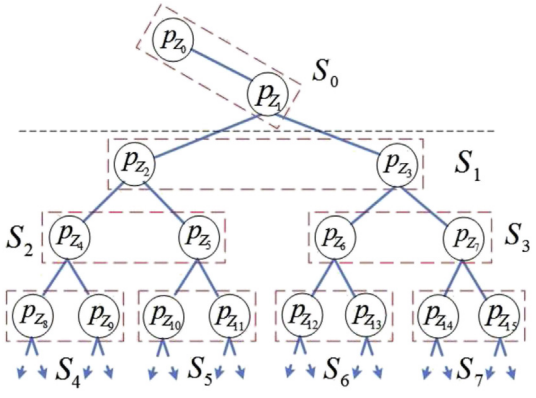

Fig. 10 – An example of dividing p_Z, where $l = 1$.

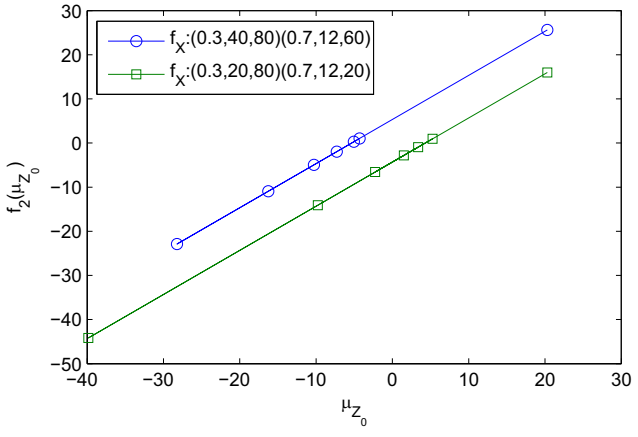

Fig. 11 – The relationship between μ_{Z_0} and f_2.

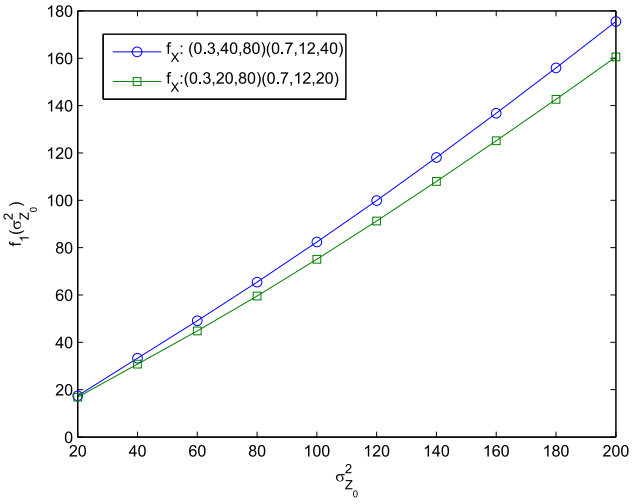

Fig. 12 – The relationship between $\sigma^2_{Z_0}$ and f_1.

subsections, we focus on some special cases, where the algorithm is much simplified (the complexity is O(1)).

Actually, this algorithm is equal to the algorithm using the first 2^L components to approximate the optimal distribution. Since only 2^l Gaussian distributions in f_{Zap}, The similar items can be merged. The code from line 16 to 20 calculates the weights of the first 2^L components and merges them.

7.2. *Case 1: the period of μ_Z is 2*

Consider a special case that the period of μ_Z is 2, i.e. $l = 1$, where Theorem 7 holds. Thus from Eq. (40)

$$S = rS_0$$

where r is a constant related to r_0(or r_1). Therefore, by normalization, $S = \{p_{Z_0}, p_{Z_1}\}$. From this conclusion, Algorithm 1 is simplified that getting stable S directly. So line 16 to 20 can be replaced by "$S = S_0$" directly.

When $t_1 \to 1$, $|\mu_{X_1} - \mu_{X_0}| \to 0$, f_x converges to Gaussian distribution, so Gaussian distribution is a near-optimal solution. In the next section, we could find this approximation is even better than Gaussian distribution.

7.3. *Case 2: $|\mu_{X_0} - \mu_{X_1}| \gg 0$*

In this case, the two components of f_x are far away from each other. Consider the general solution (Eq. (9)), which is equivalent to

$$f_Z(z) = C'\left(f_{X_0} * f_Z + f_{X_1} * f_Z\right) e^{-\lambda\left(z+\frac{\omega}{\lambda}\right)^2}, \tag{46}$$

where f_{X_0} and f_{X_1} are the expression of x_0 and x_1 respectively. The factor "$e^{-\lambda(z+\omega/\lambda)^2}$" is like a filter, which makes all the values satisfying $|z + \omega/\lambda| > 0$ close to 0. In another word, $e^{-\lambda(z+\omega/\lambda)^2}$ makes $z \notin [-L - \omega/\lambda, L - \omega/\lambda]$ be close to 0.

Algorithm 1: Calculating the Gaussian components of f_{Zap}

input : $x_0 = (p_{X_0}, \mu_{X_0}, \sigma^2_{X_0})$, $x_1 = (p_{X_1}, \mu_{X_1}, \sigma^2_{X_1})$, where $\sigma^2_{X_0} \geqslant \sigma^2_{X_1}$, σ^2_m, l, L
output: $S(= \{p_{Z_0}, p_{Z_1}, \cdots, p_{Z_{2^l-1}}\})$, $\{\mu_{Z_0}, \mu_{Z_1}, \cdots, \mu_{Z_{2^l-1}}\}$, $\{\sigma_{Z_0}, \sigma_{Z_1}, \cdots, \sigma_{Z_{2^l-1}}\}$

1 $\sigma^2_{Z_0} \leftarrow \sigma^2_m$;
2 vUpperVar0 $\leftarrow \sigma^2_m$; vLowerVar0 $\leftarrow 0$; vVar $\leftarrow 0$;
3 **while** $|vVar - \sigma^2_m| > \xi_0$ **do**
4 $\quad\mu_{Z_0} \leftarrow 0$; $p_{Z_0} \leftarrow 1$;
5 $\quad$vUpperMu0 $\leftarrow$ maxNumber; vLowerMu0 $\leftarrow$ minNumber;
6 $\quad Mu \leftarrow 1$;
7 $\quad$**while** $|Mu| > \xi_1$ **do**
8 $\quad\quad$calculate $\sigma^2_{Y_{00}}$, $\sigma^2_{Y_{01}}$ and 2λ by Eq. (24)(23);
9 $\quad\quad$calculate $\mu_{Y_{00}}$, $\mu_{Y_{01}}$ and ω by Eq. (27)(26);
10 $\quad\quad$calculate $p_{Y_{00}}$, $p_{Y_{01}}$ and C by Eq. (30)(29);
11 $\quad\quad$**for** $i = 0$ **to** $2^{l-1} - 1$ **do**
12 $\quad\quad\quad$calculate $\sigma^2_{Z_{2i}}$ and $\sigma^2_{Z_{2i+1}}$ by Eq. (24);
13 $\quad\quad\quad$calculate $\mu_{Z_{2i}}$ and $\mu_{Z_{2i+1}}$ by Eq. (27);
14 $\quad\quad\quad$calculate $p_{Z_{2i}}$ and $p_{Z_{2i+1}}$ by Eq. (30);
15 $\quad\quad$**end**
16 $\quad\quad S_0 = \{p_{Z_0}, p_{Z_1}, \cdots, p_{Z_{2^l-1}}\}$;
17 $\quad\quad$**for** $k = 1$ **to** $2^{L-l} - 1$ **do**
18 $\quad\quad\quad$calculate S_k by Eq. (40);
19 $\quad\quad$**end**
20 $\quad\quad S = \left(\sum_{i=0}^{2^{L-l}-1} S_i\right) / \mathrm{sum}\left(\sum_{i=0}^{2^{L-l}-1} S_i\right)$;
21 $\quad\quad\{p_{Z_0}, p_{Z_1}, \cdots, p_{Z_{2^l-1}}\} = S$;
22 $\quad\quad Mu \leftarrow \sum_{j=0}^{2^l-1} p_{Z_j}\mu_{Z_j}$;
23 $\quad\quad$**if** $Mu > 0$ **then**
24 $\quad\quad\quad$vUpperMu0 $\leftarrow \mu_{Z_0}$;
25 $\quad\quad$**else**
26 $\quad\quad\quad$vLowerMu0 $\leftarrow \mu_{Z_0}$;
27 $\quad\quad$**end**
28 $\quad\quad\mu_{Z_0} \leftarrow \frac{\mathrm{vUpperMu0}+\mathrm{vLowerMu0}}{2}$;
29 $\quad$**end**
30 $\quad$vVar $\leftarrow \sum_{j=0}^{2^l-1} p_{Z_j}(\sigma^2_{Z_j} + \mu^2_{Z_j})$;
31 $\quad$**if** $vVar > \sigma^2_m$ **then**
32 $\quad\quad$vUpperVar0 $\leftarrow \sigma^2_{Z_0}$;
33 $\quad$**else**
34 $\quad\quad$vLowerVar0 $\leftarrow \sigma^2_{Z_0}$;
35 $\quad$**end**
36 $\quad\sigma^2_{Z_0} \leftarrow \frac{\mathrm{vUpperVar0}+\mathrm{vLowerVar0}}{2}$;
37 **end**

Since translation of f_x does not have influence on the result, at first we transmit f_x to satisfy $\mu_{X_0} = -\omega/\lambda$. Suppose $|\mu_{X_0} - \mu_{X_1}| > (3p_{X_1}(\sigma^2_{X_1} + \sigma^2_m) + L)$ (Fig. 13). In interval $[-L - \omega/\lambda, L - \omega/\lambda]$, the values contributed by $f_{X_1} * f_Z$ is close to 0, so Eq. (46) is approximated by

$$f_Z(z) = C'\left(f_{X_0} * f_Z\right) e^{-\lambda\left(x+\frac{\omega}{\lambda}\right)^2}, \tag{47}$$

which is transmitted to the one Gaussian component problem as Section 4.2. Thus Gaussian distribution converges to the optimal solution.

8. Simulation

In this section, we inspect the performance of our methods constructing f_{Zap} to approximate the optimal noise addition distribution f_Z, especially the two special cases. min $I(X; X + Z)$ can be calculated directly by optimization problem (8). $I(X; X + Z_f)$ and $I(X; X + Z_G)$ denote the results that the data distribution is f_x, the noise distributions are f_{Zap} and Gaussian distribution respectively.

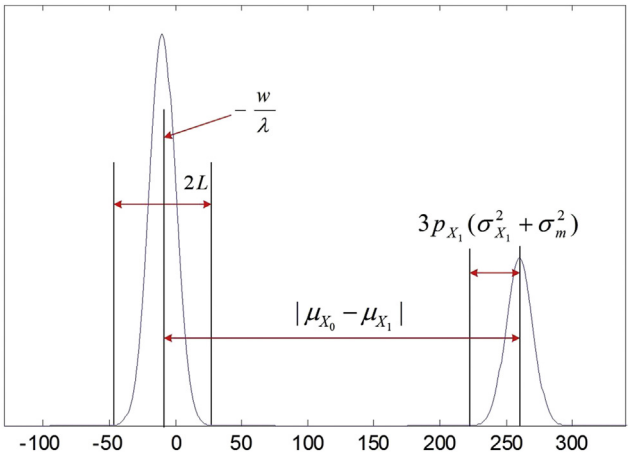

Fig. 13 – Illustration of the solution in the situation of $|\mu_{X_1}-\mu_{X_0}| \gg 0$.

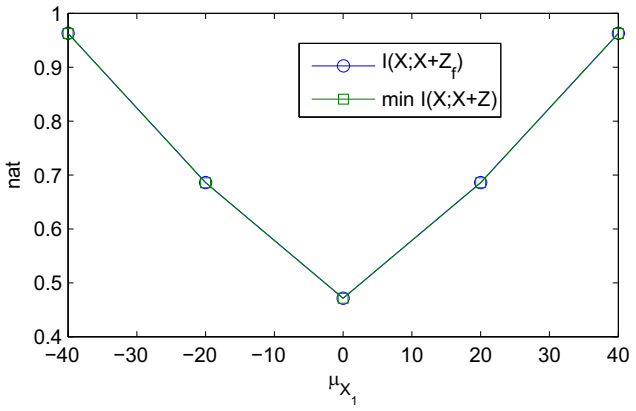

Fig. 15 – The performance of f_{Zap}, where $f_X = (0.7, 0, 100)(0.3, \mu_{X_1}, 80)$, $\sigma^2_m = 60$, $l = 4$, $L = 13$.

8.1. *Arbitrary cases*

Algorithm 1 calculates arbitrary f_x consisting of two Gaussian components. Three examples are shown in Figs. 14–16, where we change $\sigma^2_{X_1}$, μ_{X_1} and p_{X_0} respectively (we choose $l = 4$ and $L = 13$). The performance of approximation is good that only a little difference to the optimal result, regardless of the change of the parameters of f_x. From Algorithm 1, the accuracy of algorithm are based on two aspects. One is l, which is related to the period of μ_Z. Strictly speaking, the period of μ_Z is infinite. The periodicity is an approximative property. The other is L, which converges to infinite to calculate the stable weights of 2^l Gaussian functions contained in f_{Zap}. The deviation exists because of these two constraints. In Fig. 14, the maximum deviation is 0.00073 at $\sigma^2_{X_1} = 60$. The minimum deviation is 0.00052 at $\sigma^2_{X_1} = 100$. That is because with the increase of $\sigma^2_{X_1}$, the period 2^4 is more accurate. In Fig. 15, the maximum deviation is 0.00062 at $\mu_{X_1} = 40$. The minimum deviation is 0.0000003 at $\mu_{X_1} = 0$. The reason is the approximation of periodicity is more accurate when $\mu_{X_1} \to 0$ (when $\mu_{X_1} \to 0$, the period of μ_Z can be regarded as 2, so $l = 4$ is more accurate). In Fig. 16, the maximum and minimum deviations do not have the apparent rules as the former two examples. The maximum and minimum deviation are 0.00039 at $p_{X_0} = 0.5$ and 0.0000014 at $p_{X_0} = 0.9$ in our sample points. p_x is related to r_i ($i = 0, \ldots 2^l - 1$), which is more accurate when L is larger. Next we focus on two special cases, investigating the accuracy of the approximation.

8.2. *Case 1: the period of μ_Z is 2*

In this case we can only use the first 2 components to construct f_{Zap}. Fig. 17 shows the performance of f_{Zap} when $t_1 \to 1$ and $t_0 \to 0$. From the figure, t_1 is fixed (0.9), when t_0 is smaller and smaller, the deviation between f_{Zap} and the real optimal distribution is decreasing.

Fig. 18 shows the performance of f_{Zap} when $t_1 \to 1$ and $|\mu_{X_1} - \mu_{X_0}| \to 0$. Under these two constraints, f_{Zap} can be expressed by 2 Gaussian components too. f_Z performs better and better with the decrease of $|\mu_{X_1} - \mu_{X_0}|$. Actually, in this case f_x converges to Gaussian distribution, so Gaussian distribution also performs good. Fig. 19 shows the comparison of Gaussian distribution and f_{Zap}. When $|\mu_{X_1} - \mu_{X_0}| \le 15$, f_{Zap} performs better than Gaussian distribution. Particularly, when $|\mu_{X_1} - \mu_{X_0}| \le 10$, f_{Zap} and the real optimal distribution is almost the same. When $|\mu_{X_1} - \mu_{X_0}| > 15$, the condition

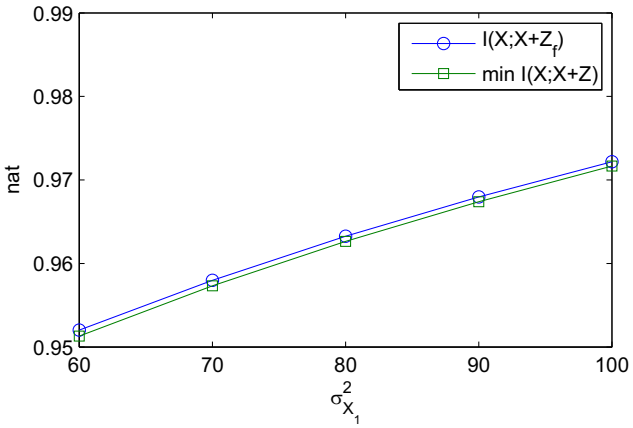

Fig. 14 – The performance of f_{Zap}, where $f_X = (0.7, 0, 100)(0.3, 40, \sigma^2_{X_1})$, $\sigma^2_m = 60$, $l = 4$, $L = 13$.

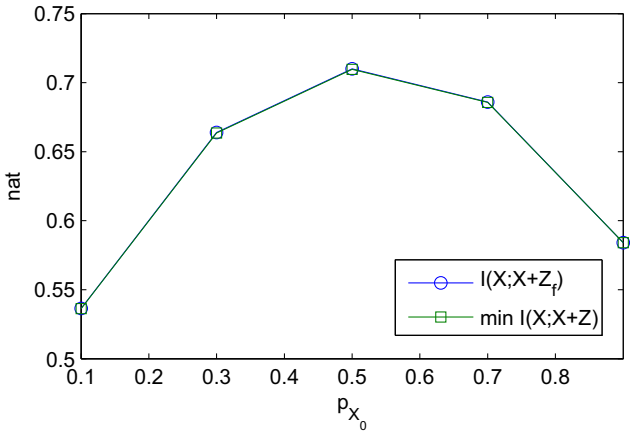

Fig. 16 – The performance of f_{Zap}, where $f_X = (p_{X_0}, 0, 100)(1 - p_{X_0}, 20, 80)$, $\sigma^2_m = 60$, $l = 4$, $L = 13$.

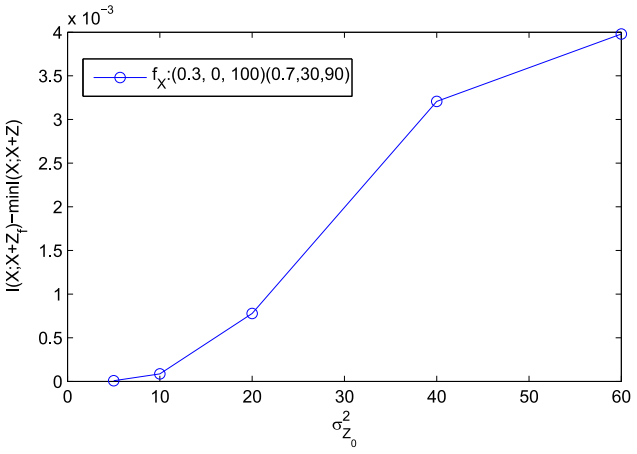

Fig. 17 – The performance of f_{Zap} when $t_1 \to 1$ and $t_0 \to 0$.

$|\mu_{X_1} - \mu_{X_0}| \to 0$ is compromised, the deviation would be larger and larger since the period of μ_Z is not 2 any more.

8.3. *Case 2:* $|\mu_{X_1} - \mu_{X_0}| \gg 0$

Fig. 20 shows the performance of f_{Zap} when $|\mu_{X_1} - \mu_{X_0}| \gg 0$. In this case, Gaussian distribution is very close to the optimal one. From the figure, when $|\mu_{X_1} - \mu_{X_0}| > 50$, $I(X; X + Z_G) - \min I(X; X + Z)$ decreases with the increase of $|\mu_{X_1} - \mu_{X_0}|$. It is because with the increase of $|\mu_{X_1} - \mu_{X_0}|$, the values of x_1 in the range 2L (determined by "$e^{-\lambda x^2 - \omega x}$", shown in Fig. 13) are smaller and smaller. From the figure, we also find out when $|\mu_{X_1} - \mu_{X_0}| < 50$, $I(X; X + Z_G) - \min I(X; X + Z)$ increases with the increase of $|\mu_{X_1} - \mu_{X_0}|$. It is because f_x is close to Gaussian distribution when $|\mu_{X_1} - \mu_{X_0}| \to 0$, where Gaussian distribution is optimal noise addition distribution.

8.4. *Comparison*

In noise addition method, some noise distributions such as Homogeneous distribution (e.g. Agrawal and Srikant, 2000)

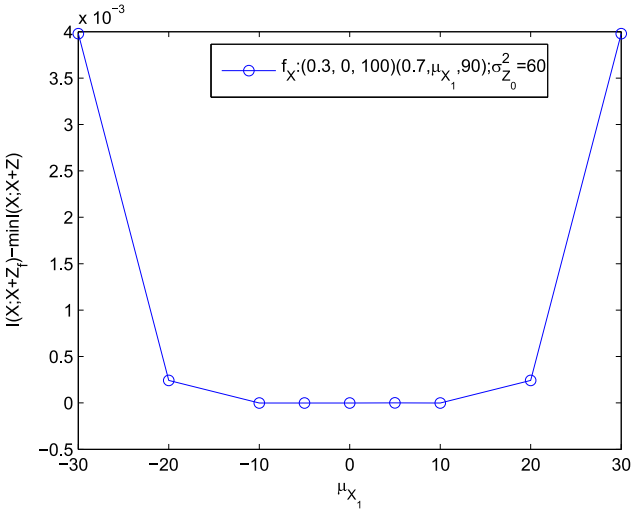

Fig. 18 – The performance of f_{Zap} when $t_1 \to 1$ and $|\mu_{X_1} - \mu_{X_0}| \to 0$.

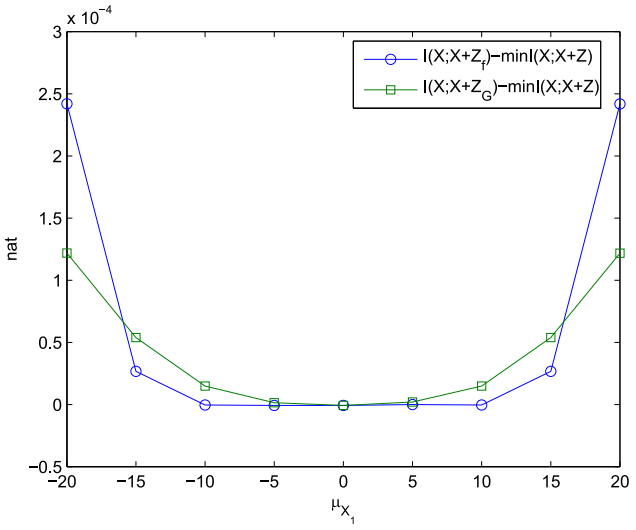

Fig. 19 – The performance of f_{Zap} and Gaussian distribution when $t_1 \to 1$ and $|\mu_{X_1} - \mu_{X_0}| \to 0$, where f_x consists of (0.3, 0, 100) and $(0.7, \mu_{X_1}, 90)$, and $\sigma^2_{Z_0} = 60$.

and Laplace distribution (e.g. Dwork, 2006) have been used. Fig. 21 shows the privacy-preserving capabilities of these three noise distributions, where f_{ap} is the approximation of optimal noise distribution from our method. From the figure, we could find that the mutual information of f_{ap}, which measures the privacy protection strength, is the smallest in these three distribution. It means that by adding the noise following the distribution function f_{ap}, the attacker gets the least information of the true value from the perturbed value.

Fig. 22 illustrates the privacy-preserving capabilities of f_{ap}, Homogeneous distribution and Laplace distribution when f_x satisfies $t_1 \to 1$ and $|\mu_{X_1} - \mu_{X_0}| \to 0 (-30 \le \mu_{X_1} \le 30)$, and $|\mu_{X_1} - \mu_{X_0}| \gg 0 (40 \le \mu_{X_1})$. In the former situation, f_{ap} can be expressed by 2 Gaussian components and be calculated in $O(1)$ times. In the letter situation, f_{ap} is Gaussian distribution. From the figure, in the two situations f_{ap} is the best one to protect the individual privacy among the three distributions.

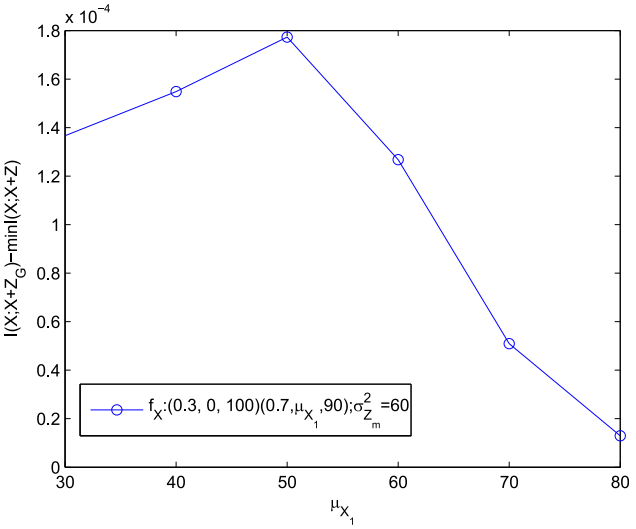

Fig. 20 – The performance of f_{Zap} when $|\mu_{X_1} - \mu_{X_0}| \gg 0$.

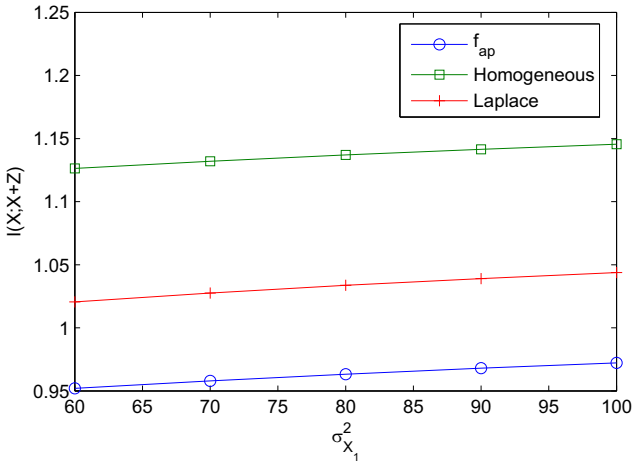

Fig. 21 – Compare the privacy-preserving capabilities of f_{ap}, Homogeneous distribution and Laplace distribution, where $f_X = (\mathbf{0.7}, \mathbf{0}, \mathbf{100})(\mathbf{0.3}, \mathbf{40}, \sigma^2_{X_1})$, $\sigma^2_m = \mathbf{60}$.

8.5. *Performance*

From Section 7.1, the complexity of Algorithm 1 is $O(2^L)$. Fig. 23 illustrates the time cost with different L. Here we calculate f_{ap} by Algorithm 1, where $f_x = (0.3, 0, 100)(0.7, -30, 60)$. The algorithm is coded by MATLAB, which runs on the notebook with Intel®Core™i5 CPU (2 × 2.40 GHZ) and 4 GB RAM. From the figure, when the larger L is chosen, the time cost grows up with exponential rate, which limits the application of the algorithm.

9. Conclusion and future work

In this paper, we quantify the accuracy of result and the privacy of individuals. Based on the metrics, we propose the optimization problem, and find out the optimal noise distribution that provides best privacy protection while maintaining the acceptable deviation from the accurate result. For the special cases that the original data of individuals follows Gaussian distribution, Gaussian distribution is the optimal result. For the general case that the original data follows arbitrary continuous distribution, the optimal solution consists of infinite number of Gaussian components. We give a way to calculate the components. By analyzing the properties of the components, the optimal distribution can be approximated by finite components. By simulation the approximation also performs good.

This paper is just the beginning. The complexity of Algorithm 1 is $O(2^L)$, which limits the algorithm when a large L is needed. That is because Algorithm 1 is based on Eq. (40), which calculate S in an iterative way. Next a non-iterative general formula is needed, which will break the shackle of L. Furthermore, the extended algorithm of Algorithm 1, with the f_x composed of multiple Gaussian components as input and the optimal noise distribution as output, is needed, which could be applied for most of the aggregation applications in practice.

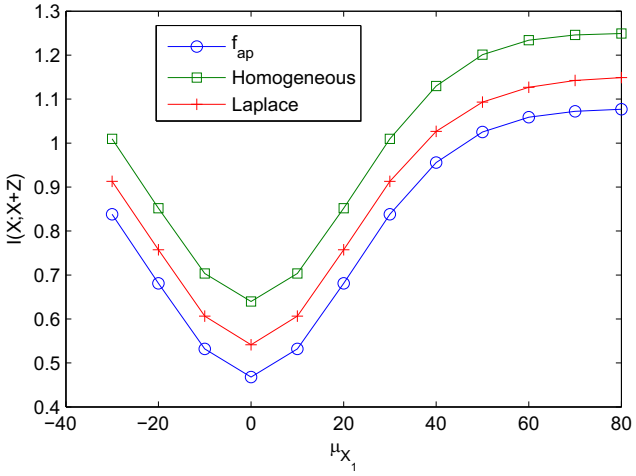

Fig. 22 – Compare the privacy-preserving capabilities of f_{ap}, Homogeneous distribution and Laplace distribution, where $f_X = (\mathbf{0.3}, \mathbf{0}, \mathbf{100})(\mathbf{0.7}, \mu_{\mathbf{X}_1}, \mathbf{90})$, $\sigma^2_m = \mathbf{60}$.

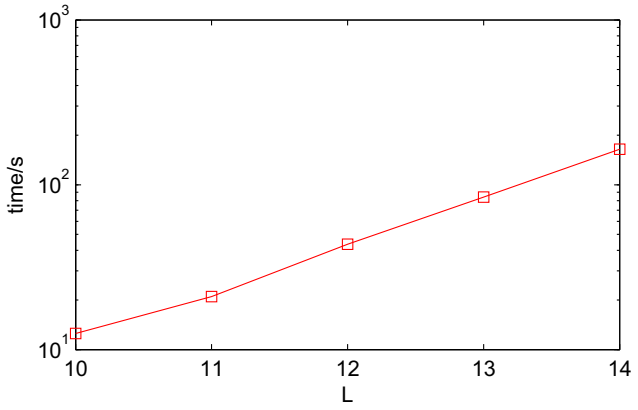

Fig. 23 – The time cost with different L.

Acknowledgments

The work was supported partly by National Natural Science Foundation of China under Grant No. 61371192, National Natural Science Foundation of China under Grant No. 61271271, 100 Talents Program of Chinese Academy of Science, the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06030601, and the Funding of Science and Technology on Information Assurance Laboratory under Grant KJ-13-003.

Appendix A. The proof of Theorem 1

Proof. Firstly we consider a more general problem

$$\begin{aligned}&\min_{f_{Y|X}(y|x)} && I(X;Y)\\ &\int\int f_X(x)f_{Y|X}(y|x)(y-x)^2\,dx\,dy \le \sigma_m^2\\ &\text{s.t.} \int f_{Y|X}(y|x)(y-x)dy = 0\\ &\int f_{Y|X}(y|x)dy = 1,\end{aligned} \tag{A.1}$$

where $Y = Z + X$. If Z is independent of X, we have

$$f_{Y|X}(y|x) = f_{Y-X|X}(y-x|x) = f_{Z|X}(z|x) = f_Z(z). \tag{A.2}$$

The constraints become

$$\int\int f_X(x)f_{Y|X}(y|x)(y-x)^2\,dx\,dy = \int f_Z(z)z^2\,dz \tag{A.3}$$

$$\int f_X(x)f_{Y|X}(y|x)(y-x)dy = \int f_Z(z)z\,dz \tag{A.4}$$

$$\int f_{Y|X}(y|x)\,dy = \int f_Z(z)\,dz. \tag{A.5}$$

This problem is translated to the problem (8). In other words, the problem (8) is a special case of the problem (A.1).

The mutual information $I(X;Y)$ is

$$\begin{aligned}I(X;Y) &= \int\int f_{X,Y}(x,y)\log\frac{f_{X,Y}(x,y)}{f_X(x)f_Y(y)}dx\,dy\\ &= \int\int f_X(x)f_{Y|X}(y|x)\log\frac{f_{Y|X}(y|x)}{f_Y(y)}dx\,dy.\end{aligned} \tag{A.6}$$

where $f_Y(y) = \int_x f_X(x)f_{Y|X}(y|x)dx$.

We use the method of Lagrange multipliers to find the solution. Set up the functional

$$\begin{aligned}J = &\int\int f_X(x)f_{Y|X}(y|x)\log\frac{f_{Y|X}(y|x)}{f_Y(y)}dydx\\ &+\lambda\int\int f_X(x)f_{Y|X}(y|x)(y-x)^2\,dy\,dx\\ &+\int u(x)\int f_{Y|X}(y|x)(y-x)dy\,dx + \int v(x)\int f_{Y|X}(y|x)dy\,dx.\end{aligned} \tag{A.7}$$

Differentiating with respect to $f_{Y|X}(y|x)$, we have

$$\begin{aligned}\frac{\partial J}{\partial f_{Y|X}(y|x)} &= f_X(x)\log\frac{f_{Y|X}(y|x)}{f_Y(y)} + f_X(x) - \int f_X(x')f_{Y|X}(y|x')\frac{1}{f_Y(y)}f_X(x)dx'\\ &\quad +\lambda f_X(x)(y-x)^2 + u(x)(y-x) + v(x)\\ &= f_X(x)\log\frac{f_{Y|X}(y|x)}{f_Y(y)} + \lambda f_X(x)(y-x)^2 + u(x)(y-x) + v(x)\\ &= 0.\end{aligned} \tag{A.8}$$

Set $\omega(x) = u(x)/f_x(x)$ and $\tau(x) = v(x)/f_x(x)$,

$$f_X(x)\left[\log\frac{f_{Y|X}(y|x)}{f_Y(y)} + \lambda(y-x)^2 + \omega(x)(y-x) + \tau(x)\right] = 0. \tag{A.9}$$

Thus

$$f_{Y|X}(y|x) = f_Y(y)e^{-\lambda(y-x)^2-\omega(x)(y-x)-\tau(x)}. \tag{A.10}$$

Here we get the expression of $f_{Y|X}(y|x)$. In problem (8), $Y = X + Z$ and Z is independent of X. From Eq. (A.10),

$$f_Z(z) = f_Y(x+z)e^{-\lambda z^2-\omega(x)z-\tau(x)}. \tag{A.11}$$

Z and X are independent, for any x, $f_Z(z)$ is unchangeable. $f_Z(z)$ can be calculated by fixing the x (e.g. $x = 0$). So $f_Z(z)$ is simplified as $f_Z(z) = f_Y(z)e^{-\lambda z^2-\omega(0)z-\tau(0)}$, where λ, $\omega(0)$ and $\tau(0)$ are constants for fixed f_x. For convenience, $\omega(0)$ and $e^{-\tau(0)}$ are abbreviated as ω and C. Therefore,

$$f_Z(z) = Cf_Y(z)e^{-\lambda z^2-\omega z} \tag{A.12}$$

□

Appendix B. The proof of Lemma 1

Proof. Since

$$\sigma_{Y_{j1}}^2 = \sigma_{Z_j}^2 + \sigma_{X_1}^2 \le \sigma_{Z_j}^2 + \sigma_{X_0}^2 = \sigma_{Y_{j0}}^2, \tag{B.1}$$

we have

$$\frac{1}{\sigma_{Z_{2j+1}}^2} = \frac{1}{\sigma_{Y_{j1}}^2} + 2\lambda \ge \frac{1}{\sigma_{Y_{j0}}^2} + 2\lambda = \frac{1}{\sigma_{Z_{2j}}^2}. \tag{B.2}$$

So $\sigma_{Z_{2j}}^2 \ge \sigma_{Z_{2j+1}}^2$. The equation holds when $\sigma_{X_0}^2 = \sigma_{X_1}^2$. □

Appendix C. The proof of Lemma 2

Proof. For $j = 0$, $\sigma_{Z_{2j}}^2 = \sigma_{Z_j}^2$.

For $j \in \mathbb{N}^+$, from Eq. (24) we have

$$\begin{aligned}\frac{\sigma_{Z_j}^2}{\sigma_{Z_{2j}}^2} &= \frac{\sigma_{Z_j}^2}{\sigma_{Z_j}^2+\sigma_{X_0}^2} + 2\lambda\sigma_{Z_j}^2 = 1 - \frac{\sigma_{X_0}^2}{\sigma_{Z_j}^2+\sigma_{X_0}^2} + \frac{\sigma_{X_0}^2\sigma_{Z_j}^2}{\sigma_{Z_0}^2\left(\sigma_{Z_0}^2+\sigma_{X_0}^2\right)}\\ &= 1 + \frac{\sigma_{X_0}^2\left(\sigma_{Z_j}^2-\sigma_{Z_0}^2\right)\left(\sigma_{Z_j}^2+\sigma_{Z_0}^2+\sigma_{X_0}^2\right)}{\sigma_{Z_0}^2\left(\sigma_{Z_0}^2+\sigma_{X_0}^2\right)\left(\sigma_{Z_j}^2+\sigma_{X_0}^2\right)} \overset{(a}{\le} 1\end{aligned} \tag{C.1}$$

where (a) follows from $\sigma_{Z_j}^2 \le \sigma_{Z_0}^2$. So $\sigma_{Z_{2j}}^2 \ge \sigma_{Z_j}^2$. The equation holds when $\sigma_{Z_j}^2 = \sigma_{Z_0}^2$. □

Appendix D. The proof of Theorem 3

Proof. Consider the series

$$\left(\frac{1}{2\lambda+\frac{1}{\sigma_{X_1}^2}}, \frac{1}{2\lambda+\frac{1}{\sigma_{X_1}^2+\frac{1}{2\lambda+\frac{1}{\sigma_{X_1}^2}}}}, \cdots\right)$$

denoted by $(s_1, s_2, \ldots)$. Since

$$s_k = \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_1} + \frac{1}{\cdots + \frac{1}{\sigma^2_{X_1}}}}} \tag{D.1}$$

and

$$s_{k+1} = \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_1} + \frac{1}{\cdots + \frac{1}{\sigma^2_{X_1} + \gamma_k}}}} \tag{D.2}$$

where $\gamma_k = 1/2\lambda + 1/\sigma^2_{X_1} > 0$, we have $s_{k+1} > s_k$. Since

$$s_{k+1} = \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_1} + s_k}}, \tag{D.3}$$

we have

$$\lim_{k\to+\infty} s_k = \frac{\sqrt{\lambda^2\sigma^4_{X_1} + 2\lambda\sigma^2_{X_1}} - \lambda\sigma^2_{X_1}}{2\lambda} = \frac{1}{2}\left(\sqrt{\sigma^4_{X_1} + \frac{2}{\lambda}\sigma^2_{X_1}} - \sigma^2_{X_1}\right), \tag{D.4}$$

denoted by s_∞. Then we compare s_∞ and $\sigma^2_{Z_0}$. Since

$$\sqrt{\sigma^4_{X_1} + \frac{2}{\lambda}\sigma^2_{X_1}} = \sqrt{\sigma^4_{X_1} + 4\frac{\sigma^2_{X_1}}{\sigma^2_{X_0}}\sigma^4_{Z_0} + 4\sigma^2_{X_1}\sigma^2_{Z_0}} \tag{D.5}$$
$$\le \sqrt{\sigma^4_{X_1} + 4\sigma^4_{Z_0} + 4\sigma^2_{X_1}\sigma^2_{Z_0}} = \sigma^2_{X_1} + 2\sigma^2_{Z_0},$$

we have

$$s_\infty \le \sigma^2_{Z_0}, \tag{D.6}$$

where the equation holds when $\sigma^2_{X_0} = \sigma^2_{X_1}$. Therefore, for any $\sigma^2_{Z_j}$,

$$\sigma^2_{Z_{(j_0 j_1 \cdots j_t)}} = \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_{j_t}} + \frac{1}{\cdots + \frac{1}{\sigma^2_{X_{j_0}} + \sigma^2_{Z_0}}}}} \ge \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_1} + \frac{1}{\cdots + \frac{1}{\sigma^2_{X_1} + s_\infty}}}} = s_\infty \tag{D.7}$$

Thus $s_\infty \le \sigma^2_{Z_j} \le \sigma^2_{Z_0}$. When $\sigma^2_{X_0} = \sigma^2_{X_1}$, $s_\infty = \sigma^2_{Z_0}$. □

Appendix E. The proof of Lemma 3

Proof. From Eq. (24) for $j \in \mathbb{N}$ we have

$$\frac{\sigma^2_{Z_j}}{\sigma^2_{Z_{2j+1}}} = \frac{\sigma^2_{Z_j}}{\sigma^2_{Z_j} + \sigma^2_{X_1}} + 2\lambda\sigma^2_{Z_j} = 1 + \frac{2\lambda\sigma^2_{Z_j}\left(\sigma^2_{Z_j} + \sigma^2_{X_1}\right) - \sigma^2_{X_1}}{\sigma^2_{Z_j} + \sigma^2_{X_1}}$$
$$= 1 + \frac{2\lambda\left(\sigma^2_{Z_j}\right)^2 + 2\lambda\sigma^2_{Z_j}\sigma^2_{X_1} - \sigma^2_{X_1}}{\sigma^2_{Z_j} + \sigma^2_{X_1}}. \tag{E.1}$$

Consider the quadratic function of $\sigma^2_{Z_j}$

$$F\left(\sigma^2_{Z_j}\right) = 2\lambda\left(\sigma^2_{Z_j}\right)^2 + 2\lambda\sigma^2_{Z_j}\sigma^2_{X_1} - \sigma^2_{X_1}, \tag{E.2}$$

when $\sigma^2_{Z_j} \ge \sqrt{\lambda^2\sigma^4_{X_1} + 2\lambda\sigma^2_{X_1}} - \lambda\sigma^2_{X_1}/2\lambda = s_\infty$, $F(\sigma^2_{Z_j}) \ge 0$. According to Theorem 3, this relationship holds. Thus $\sigma^2_{Z_j} \ge \sigma^2_{Z_{2j+1}}$. The equation holds when $\sigma^2_{Z_j} = s_\infty$. □

Appendix F. The proof of Lemma 4

Proof. For any $j \in [2^t, 2^{t+1})$, $t > 0$ j can be expressed as $(j_0, j_1, \ldots, j_t)$, where $j_0 = 1$.

$$\sigma^2_{Z_{(j_0, j_1, \cdots, j_t)}} = \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_{j_t}} + \frac{1}{\cdots + \frac{1}{\sigma^2_{X_{j_0}} + \sigma^2_{Z_0}}}}}$$
$$\le \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_0} + \frac{1}{\cdots + \frac{1}{\sigma^2_{X_1} + \sigma^2_{Z_0}}}}} = \sigma^2_{Z_{(1,0,0,\cdots,0)}} = \sigma^2_{Z_{2^t}}. \tag{F.1}$$

If j is even, $j_t = 0$, we have

$$\sigma^2_{Z_{(j_0 j_1 \ldots j_t)}} \ge \sigma^2_{Z_{(1,1,\ldots,1,0)}} = \sigma^2_{Z_{2^{t+1}-2}}. \tag{F.2}$$

Similarly,

$$\sigma^2_{Z_{(j_0 j_1 \ldots j_t)}} \ge \sigma^2_{Z_{(1,1,1,\ldots,1)}} = \sigma^2_{Z_{2^{t+1}-1}}. \tag{F.3}$$

If j is add, $j_t = 1$, we have

$$\sigma^2_{Z_{(j_0 j_1 \ldots j_t)}} \le \sigma^2_{Z_{(1,0,\ldots,0,1)}} = \sigma^2_{Z_{2^t+1}}. \tag{F.4}$$

□

Appendix G. The proof of Lemma 5

Proof. Suppose j is even, and $j \in \mathbb{N}^+$. From Lemma 2 and Lemma 4 we know $(\sigma^2_{Z_{2^1}}, \sigma^2_{Z_{2^2}}, \ldots, \sigma^2_{Z_{2^t}}, \ldots)$, each of which is the largest variance with even indices in its level, is a non-decreasing sequence. Thus the $\max\sigma^2_{Z_j} = \lim_{t\to\infty}\sigma^2_{Z_{2^t}}$, and

$$\max\ \sigma^2_{Z_j} = \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_0} + \max\ \sigma^2_{Z_j}}}, \tag{G.1}$$

from which we have

$$\max\ \sigma^2_{Z_j} = \sigma^2_{Z_0}. \tag{G.2}$$

Consider the sequence $(\sigma^2_{Z_0}, \sigma^2_{Z_2}, \ldots, \sigma^2_{Z_{2^{t+1}-2}}, \ldots)$, each of which is the smallest variance with even indices in its level. Since

$$2\lambda + \frac{1}{\sigma^2_{X_0} + \sigma^2_{Z_{2^{t+1}-2}}} = \frac{1}{\sigma^2_{Z_{2^t-1}}} \overset{(a}{\le} \frac{1}{\sigma^2_{Z_{2^{t+1}-1}}} = 2\lambda + \frac{1}{\sigma^2_{X_0} + \sigma^2_{Z_{2^{t+2}-2}}}, \tag{G.3}$$

where (a) follows from Lemma 3, we have

$$\sigma^2_{Z_{2^{t+1}-2}} \ge \sigma^2_{Z_{2^{t+2}-2}} \tag{G.4}$$

for any $j \in \mathbb{N}$. Thus the sequence is a non-increasing sequence, from which we have $\min\sigma^2_{Z_j} = \lim_{t\to\infty}\sigma^2_{Z_{2^{t+1}-2}}$. So

$$\min\ \sigma^2_{Z_j} = \lim_{t\to\infty}\sigma^2_{Z_{2^{t+1}-2}} = \frac{1}{2\lambda + \frac{1}{\sigma^2_{X_0} + s_\infty}}. \tag{G.5}$$

Similarly, for any $j \in \mathbb{N}^+$, if j is odd, we have

$$\max\sigma_{Z_j}^2 = \sigma_{Z_1}^2 \tag{G.6}$$

$$\min\sigma_{Z_j}^2 = s_\infty \tag{G.7}$$

□

Appendix H. The proof of Theorem 4

Proof. From Lemma 5 σ_Z^2 with odd indices are in one interval, and σ_Z^2 with even indices are in another interval. The ratio of maximum of the interval of variances with odd indices to minimum is

$$\frac{\sigma_{Z_1}^2}{s_\infty} = \frac{(t_0+t_1)\left(\sqrt{t_1^2+4t_0(t_0+1)t_1}+t_1\right)}{2(t_0^2+2t_0+t_1)t_1}. \tag{H.1}$$

When $t_1 \to 1$, the ratio converges to 1. Shown in Fig. 6, when $\sigma_{X_0}^2$ is not much larger than $\sigma_{X_1}^2$, $\sigma_{Z_1}^2/s_\infty$ is close to 1, i.e. all the variances with odd indices can be regarded as the same. The ratio of maximum of the interval of variances with even indices to minimum is

$$\frac{\sigma_{Z_0}^2}{\frac{1}{2\lambda+\frac{1}{\sigma_{X_0}^2+s_\infty}}} = \frac{1}{t_0+1}+\frac{2t_0}{\sqrt{t_1^2+4t_0t_1(t_0+1)}-t_1+2}. \tag{H.2}$$

When $t_1 \to 1$, the ratio converges to 1. The same result is shown by Fig. 7 for the variances with even indices. □

Appendix I. The proof of Lemma 6

Proof. For $l > 1$, $2^l \equiv 0 \bmod 4$, $\mu_{Z_{2^l}}$ and $\mu_{Z_{2^{l+1}}}$ satisfy Eq. (33). Since $h_0 < 1$, when $l \to \infty$, $\mu_{Z_{2^l}}$ reaches a steady value, i.e. $\mu_{Z_{2^l}} = \mu_{Z_{2^{l+1}}}$. From Eq. (33) we have

$$\mu_{Z_{2^l}} = h_0\mu_{Z_{2^l}} + (1-h_0)\mu_{Z_0},$$

so

$$\mu_{Z_{2^l}} = \mu_{Z_{2^{l+1}}} = \mu_{Z_0}.$$

Similarly, from Eq. (36), we have

$$\mu_{Z_{2^{l+1}-1}} = \mu_{Z_{2^{l+2}-1}} = \frac{H_3}{1-h_3}.$$

□

Appendix J. The proof of Lemma 7

Proof. From Eqs. (33)–(36), any μ_{Z_j} at level l, $j \in [2^{l-1}, 2^l)$, can be represented in the way as

$$\mu_{Z_j} = h_{i_0}h_{i_1}\cdots h_{i_{l-1}}\mu_{Z_0} + H_j, \tag{J.1}$$

where

$$H_j = \sum_{k=0}^{l-2} H_{i_k}\sum_{t=k+1}^{l-1} h_{i_t} + H_{i_{l-1}}$$

and $i_0, i_1, \ldots, i_l \in \{0, 1, 2, 3\}$. Since $0 < h_0, h_1, h_2, h_3 < 1$, we have

$$\lim_{l\to\infty} h_{i_0}h_{i_1}\cdots h_{i_l} = 0,$$

which means when $l \to \infty$, μ_{Z_j} is only decided by h_i and H_i, $i = 0, 1, 2, 3$, not by μ_{Z_0} (there are two "μ_{Z_0}" in Eq. (J.1). This "μ_{Z_0}" is a variable in "$h_{i_0}h_{i_1}\cdots h_{i_l}\mu_{Z_0}$", which is the root of the tree. Another "μ_{Z_0}" is a constant in H_j, which actually is a part of ω. If ω is fixed, the "μ_{Z_0}" in H_j are fixed). Thus no matter what the root μ_{Z_0} is, μ_{Z_j} at level l ($l \to \infty$) is the same.

Specially, when t_0 is close to 0, in Eq. (J.1) $h_{i_0}h_{i_1}\cdots h_{i_{l-1}} \to \infty$ even when l is a small number. □

Appendix K. The proof of Theorem 5

Proof. Suppose $l = 2l_1$, where l_1 is large enough to satisfy Lemma 6 and Lemma 7. We will prove the two sequences $\{\mu_{Z_0}, \mu_{Z_1}, \ldots, \mu_{Z_{2^l-1}}\}$ and $\{\mu_{Z_{2^l}}, \mu_{Z_{2^l+1}}, \ldots, \mu_{Z_{2^{l+1}-1}}\}$ are the same.

Each sequence has 2^l elements. We divide the elements into two parts, and consider each part respectively, where $d_1 = 2^{l_1} - 1$.

1) $\{\mu_{Z_0}, \ldots, \mu_{Z_{d_1}}\}$ and $\{\mu_{Z_{2^l}}, \ldots, \mu_{Z_{2^l+d_1}}\}$.

From Lemma 6 we have $\mu_{Z_{2^{l_1}}} = \mu_{Z_{2^{l_1+1}}} = \cdots = \mu_{Z_{2^l}} = \mu_{Z_0}$, and $2^{l_1} \equiv 2^{l_1+1} \equiv \cdots 2^l \equiv 0 \bmod 4$. Consider the right subtree of μ_{Z_0}, μ_{Z_1} is the right child of μ_{Z_0}, $\mu_{Z_{2^l+1}}$ is the right child of $\mu_{Z_{2^l-1}}$. So $\mu_{Z_1} = \mu_{Z_{2^l+1}}$. μ_{Z_2} and μ_{Z_3} are the second level right children of μ_{Z_0}. $\mu_{Z_{2^l+2}}$ and $\mu_{Z_{2^l+3}}$ are the second level right children of $\mu_{Z_{2^l-2}}$. So $\mu_{Z_2} = \mu_{Z_{2^l+2}}$ and $\mu_{Z_3} = \mu_{Z_{2^l+3}}$. In this way we pair all the other nodes which are at the level less than l_1. So the two subsequences are equal.

2) $\{\mu_{Z_{d_1+1}}, \ldots, \mu_{Z_{2^l-1}}\}$ and $\{\mu_{Z_{2^l+d_1+1}}, \ldots, \mu_{Z_{2^{l+1}-1}}\}$.

$\mu_{Z_{d_1+1}}, \ldots, \mu_{Z_{2^l-1}}$ are the right children at the level l_1 to l of μ_{Z_0}. Consider any level l_2, where $(l_1 \le l_2 \le l)$, the nodes are $\{\mu_{Z_{2^{l_2}-1}}, \ldots, \mu_{Z_{2^{l_2}-1}}\}$, which are the l_2-th level right children of μ_{Z_0}. The corresponding sets $\{\mu_{Z_{2^l+2^{l_2}-1}}, \ldots, \mu_{Z_{2^l+2^{l_2}-1}}\}$ are the l_2-th level right children of $\mu_{Z_{2^{l-l_2}}}$. Since $l_1 \le l_2$, from Lemma 7 we know $\{\mu_{Z_{2^{l_2}-1}}, \ldots, \mu_{Z_{2^{l_2}-1}}\}$ equals to $\{\mu_{Z_{2^l+2^{l_2}-1}}, \ldots, \mu_{Z_{2^l+2^{l_2}-1}}\}$. So we can find the two subsequences are equal.

From above it shows the two sequences are the same. So 2^l is the period of μ_Z. □

Appendix L. The proof of Theorem 6

Proof. For $l' = l$, consider the $(2i+b)$-th elements $p_{Z_{2i+b}}$ and $p_{Z_{2^{l+1}+2i+b}}$ in the two sequences respectively, where $i = 0, 1, \ldots, 2^l - 1$, and $b = 0, 1$. We have

$$p_{Z_{2i+b}} = C\sigma_{Z_{2i+b}}\frac{p_{Z_i}p_{X_b}}{\sqrt{\sigma_{Z_i}^2+\sigma_{X_b}^2}}\cdot e^{\frac{\mu_{Z_{2i+b}}^2}{2\sigma_{Z_{2i+b}}^2}-\frac{(\mu_{X_b}+\mu_{Z_i})^2}{2\left(\sigma_{X_b}^2+\sigma_{Z_i}^2\right)}} \tag{L.1}$$

$$p_{Z_{2^{l+1}+2i+b}} = C\sigma_{Z_{2^{l+1}+2i+b}} \frac{p_{Z_{2^l+i}} p_{X_b}}{\sqrt{\sigma^2_{Z_{2^l+i}} + \sigma^2_{X_b}}} \cdot e^{\frac{\mu^2_{Z_{2^{l+1}+2i+b}}}{2\sigma^2_{Z_{2^{l+1}+2i+b}}} - \frac{\left(\mu_{X_b}+\mu_{Z_{2^l+i}}\right)^2}{2\left(\sigma^2_{X_b}+\sigma^2_{Z_{2^l+i}}\right)}}. \quad \text{(L.2)}$$

So

$$\frac{p_{Z_{2^{l+1}+2i+b}}}{p_{Z_{2i+b}}} = \frac{p_{Z_{2^l+i}}}{p_{Z_i}}, \quad \text{(L.3)}$$

Similarly, for any $l' \geq l$ and $i = 0, 1, \ldots, 2^{l'} - 1$,

$$\frac{p_{Z_{2^{l'+1}+2i+b}}}{p_{Z_{2i+b}}} = \frac{p_{Z_{2^{l'}+i}}}{p_{Z_i}}. \quad \text{(L.4)}$$

□

Appendix M. The proof of Theorem 7

Proof. From Eq. (L.1), r_0 and r_1 are

$$r_0 = \frac{p_{Z_2}}{p_{Z_0}} = \frac{p_{Z_1}}{p_{Z_0}} e^{-\frac{\left(\mu_{X_0}+\mu_{Z_1}\right)^2}{2\left(\sigma^2_{X_0}+\sigma^2_{Z_1}\right)} + \frac{\left(\mu_{X_0}+\mu_{Z_0}\right)^2}{2\left(\sigma^2_{X_0}+\sigma^2_{Z_0}\right)}}, \quad \text{(M.1)}$$

$$r_1 = \frac{p_{Z_3}}{p_{Z_1}} = \frac{p_{Z_1}}{p_{Z_0}} e^{-\frac{\left(\mu_{X_1}+\mu_{Z_1}\right)^2}{2\left(\sigma^2_{X_1}+\sigma^2_{Z_1}\right)} + \frac{\left(\mu_{X_1}+\mu_{Z_0}\right)^2}{2\left(\sigma^2_{X_1}+\sigma^2_{Z_0}\right)}}. \quad \text{(M.2)}$$

From Theorem 3, $\sigma^2_{X_0} = \sigma^2_{X_1}$ and $\sigma^2_{Z_0} = \sigma^2_{Z_1} = \cdots$, so

$$r_0 = \frac{p_{Z_1}}{p_{Z_0}} e^{\frac{\left(\mu_{Z_0}-\mu_{Z_1}\right)\left(\mu_{Z_0}+\mu_{Z_1}+2\mu_{X_0}\right)}{2\left(\sigma^2_{X_0}+\sigma^2_{Z_0}\right)}}, \quad \text{(M.3)}$$

$$r_1 = \frac{p_{Z_1}}{p_{Z_0}} e^{\frac{\left(\mu_{Z_0}-\mu_{Z_1}\right)\left(\mu_{Z_0}+\mu_{Z_1}+2\mu_{X_1}\right)}{2\left(\sigma^2_{X_0}+\sigma^2_{Z_0}\right)}}. \quad \text{(M.4)}$$

Thus

$$\frac{r_0}{r_1} = e^{\frac{\left(\mu_{Z_0}-\mu_{Z_1}\right)\left(\mu_{X_0}-\mu_{X_1}\right)}{\sigma^2_{X_0}+\sigma^2_{Z_0}}}. \quad \text{(M.5)}$$

So if $|\mu_{X_1} - \mu_{X_0}| \to 0$ or $|\mu_{Z_1} - \mu_{Z_0}| \to 0$, $r_0 = r_1$. □

REFERENCES

Adam NR, Worthmann JC. Security-control methods for statistical databases: a comparative study. ACM Comput Surv 1989;21:515–56.

Agrawal D, Aggarwal CC. On the design and quantification of privacy preserving data mining algorithms. In: 20th ACM SIGMOD-SIGACT-SIGART symposium on principles of database systems; 2001.

Agrawal R, Srikant R. Privacy-preserving data mining. In: SIGMOD; 2000.

Bezzi M. An information theoretic approach for privacy metrics. Trans Data Priv 2010;3:199–215.

Clifton C, Kantarcioglu M, Vaidya J, Lin X, Zhu MY. Tools for privacy preserving distributed data mining. ACM SIGKDD Explor Newsl 2002;4.

Cover TM, Thomas JA. Elements of information theory. 2nd ed.. Wiley-Interscience; 2006.

Domingo-Ferrer J, Seb'e F, Castell'a-Roca J. On the security of noise addition for privacy in statistical databases. In: Privacy in statistical databases; 2004. pp. 149–61.

Dwork C. Differential privacy. In: Proceedings of the 33rd international conference on automata, languages and programming – volume part II; 2006. pp. 1–12.

Dwork C, Kenthapadi K, McSherry F, Mironov I, Naor M. Our data, ourselves: privacy via distributed noise generation. In: 24th Annual international conference on the theory and applications of cryptographic techniques; 2006.

Eisenman SB, Miluzzo E, Lane ND, Peterson RA, Ahn GS, Campbell AT. The case for VM-based cloudlets in mobile computing. ACM Trans Sens Netw 2009;6.

Ghosh A, Roughgarden T, Sundararajan M. Universally utility-maximizing privacy mechanisms. In: STOC'09 proceedings of the 41st annual ACM symposium on theory of computing; 2009.

Ghosh A, Roughgarden T, Sundararajan M. Universally utility-maximizing privacy mechanisms. http://theory.stanford.edu/~tim/papers/priv.pdf; 2011.

Hanson MA. Invexity and the Kuhn–Tucker theorem. J Math Anal Appl 1999;236:594–604.

Hull B, Bychkovsky V, Zhang Y, Chen K, Michel Goraczko AM, Shih E, et al. Cartel: a distributed mobile sensor computing system. In: Proceedings of the 4th ACM international conference on embedded networked sensor systems; 2006.

Jung T, Mao X, Li XY, Tang SJ, Gong W, Zhang L. Data aggregation without secure channel: multivariate polynomial evaluation. In: infocom 2013; 2013.

Lindeberg JW. Wikipedia: central limit theorem. http://en.wikipedia.org/wiki/Central_limit_theorem.

Oliveira SRM, Zaiane OR. Privacy preserving clustering by data transformation. In: The 18th Brazilian symposium on databases; 2003.

Popa RA, Blumberg AJ, Balakrishnan H. Privacy and accountability for location-based aggregate statistics. In: CCS'11; 2011.

Rachlin Y, Probst K, Ghani R. Maximizing privacy under data distortion constraints in noise perturbation methods. In: Privacy, security, and trust in KDD; 2009. pp. 92–110.

Shi E, Chan THH, Rieffel E, Chow R, Song D. Privacy-preserving aggregation of time-series data. In: Network & distributed system security symposium (NDSS); 2011.

Su C, Bao F, Zhou J, Takagi T, Sakurai K. A new scheme for distributed density estimation based privacy-preserving clustering. In: The third international conference on availability, reliability and security; 2008.

Traub JF, Yemini Y, Wozniakowski H. The statistical security of a statistical database. ACM Trans Database Syst 1984;9:672–9.

Zhu Y, Liu L. Optimal randomization for privacy preserving data. In: KDD'04; 2004.

Hao Zhang received his B.Eng. degree in information security from University of Science and Technology of China (USTC), Hefei, in 2005. He is currently a Ph.D. candidate at School of Information Science and Technology, University of Science and Technology of China. His research interest focuses on privacy protection, mobile security, and P2P network.

Nenghai Yu received the B.S. degree in 1987 from Nanjing University of Posts and Telecommunications, the M.E. degree in 1992 from Tsinghua University, and the Ph.D. degree in 2004 from University of Science and Technology of China, where he is currently a professor. His research interests include security and privacy in mobile networks, multimedia security, multimedia information retrieval, and information hiding.

Yonggang Wen received the Ph.D. degree in electrical engineering and computer science from the Massachusetts Institute of

Technology, Cambridge, MA, USA, in 2008. He is currently an Assistant Professor with the School of Computer Engineering, Nanyang Technological University, Singapore. Previously, he was with Cisco, San Jose, CA, USA, as a Senior Software Engineer and a System Architect for content networking products. His current research interests include cloud computing, mobile computing, cyber security, multimedia networks, and green ICT.

Weiming Zhang received the M.S. and Ph.D. degrees in 2002 and 2005, respectively, from the Zhengzhou Information Science and Technology Institute, China. Currently, he is an associate professor with the School of Information Science and Technology, University of Science and Technology of China. His research interests include information hiding, multimedia security, and privacy-preserving data searching and analysis.