JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 24 No. 11, pp. 109-117, November 2019
https://doi.org/10.9708/jksci.2019.24.11.109

A Study on an Efficient and Robust Differential Privacy Scheme Using a Tag Field in Medical Environment

Soon-Seok Kim*

*Associate Professor, Dept. of Computer Engineering, Halla University, Wonju, Korea

[Abstract]

Recently, the invasion of privacy in medical information has been issued following the interest in the secondary use of mass medical information. The mass medical information is very useful information that can be used in various fields such as disease research and prevention. However, due to privacy laws such as the Privacy Act and Medical Law, this information, including patients' or health professionals' personal information, is difficult to utilize as a secondary use of mass information. To do these problem, various methods such as k-anonymity, l-diversity and differential-privacy that can be utilized while protecting privacy have been developed and utilized in this field. In this paper, we discuss the differential privacy processing of the various methods that have been studied so far, and discuss the problems of differential privacy using Laplace noise and the previously proposed differential privacy. Finally, we propose a new scheme to solve the existing problem by adding a 1-bit status field to the last column of a given data set to confirm the response to queries from analysts.

▸ **Key words**: De-identification, Differential Privacy, Medical Information, Privacy Protection, Tag.

[요 약]

최근 의료분야에서 대용량 의료정보의 이차적인 활용에 관심이 대두되고 있다. 대용량 의료정보의 경우 질병에 대한 연구나 예방 등에 활용되어 의료분야의 발전에 기여할 수 있는 유용한 정보이다. 그러나 개인정보보호법이나 의료법 등으로 인해, 의료정보는 환자나 의료진 등의 개인정보를 포함하고 있기 때문에 이차적인 활용에 많은 제한이 발생한다. 이러한 문제를 해결하기 위해 현재까지 k-익명성[1], l-다양성[2], 그리고 차분 프라이버시[3] 등 다양한 방법들이 제안되어 왔다. 본 논문에서는 지금까지 연구된 다양한 방법들 중 라플라스 노이즈를 이용한 그리고 이전에 제안된 차분 프라이버시 방법들의 문제점들에 대해 논의해보고자 한다. 끝으로 우리는 분석가들로부터의 질의에 대한 응답을 확인하기 위해 주어진 데이터 집합의 마지막 컬럼에 1 비트의 상태 필드를 추가하여 기존의 문제점을 해결하는 새로운 방법에 대해 제안해 보고자 한다.

▸ **주제어**: 할당량, 작업량, 이송, 부하균형, 시뮬레이션

• First Author: Soon-Seok Kim, Corresponding Author: Soon-Seok Kim
*Soon-Seok Kim (sskim@halla.ac.kr), Dept. of Computer Engineering, Halla University
• Received: 2019. 08. 21, Revised: 2019. 10. 14, Accepted: 2019. 10. 14.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction Introduction

Recently, attention to the secondary utilization of mass medical information has been focused on the medical field. In the case of mass medical information, it is useful information because it contributes to the development of the medical field by being utilized for research and the prevention of diseases. However, in spite of this advantage, since medical information includes the personal information of the patient or the medical staff, there are many restrictions on the secondary utilization. To solve this problem, various methods such as k-anonymity[1], l-diversity[2], and differential privacy[3] have been proposed. However, since privacy and the use of medical information are an antinomy relation, previous methods do not fully protect privacy. In this regard, a new protocol has been proposed that improves the safety and efficiency of the differential privacy scheme, which is well known as a de-identification privacy model, in a paper [4] published by Kim et al. However, in the case of the previously proposed method[4], there is an advantage that it is possible to prevent the conspiracy for the number of K and usability of the data, but there are disadvantages including the pre-distribution according to the use of the secret sharing technique, the symmetric encryption-decryption process, update to shared secret key and a calculation process of finding secret information S through Lagrange interpolation[5] is additionally generated, which results in a deterioration in efficiency. In this paper, we would like to solve this drawback by adding a 1-bit tag field, which is a status field, to the last column of a given dataset in the privacy guard database. At this time, the tag field performs the role of checking whether all records containing individual patient medical information in the requested data set from the analysts are responded / provided.

In Section Ⅱ of this paper, we will discuss existing differential privacy methods and their problems as related research. In Section Ⅲ, we propose a new method to improve these problems and analyze the safety, and then we describe the conclusion and future direction of the research in Section Ⅳ.

II. Related works

1. Differential privacy method[3]

First, the processing procedure of differential privacy in the general environment of online interactive[6] is as follows (see Fig. 1).

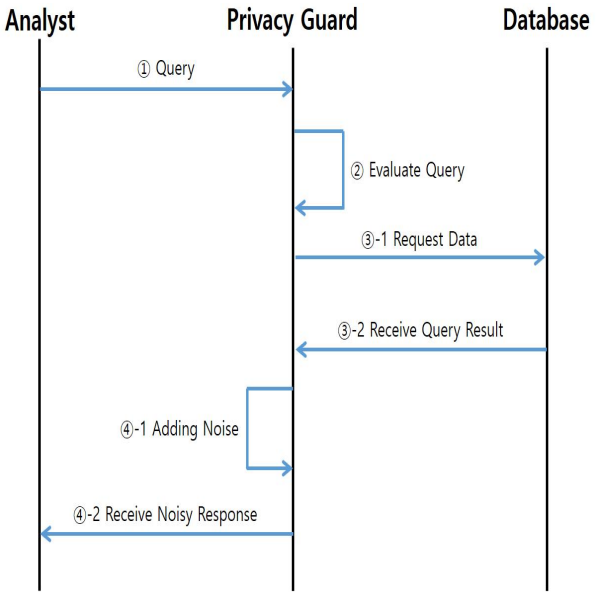

Fig. 1. Differential Privacy Process

[*Step 1: Query*] The analyst asks the intermediary software called the differential privacy guard for a query

[*Step 2: Evaluate Query*] The differential privacy guard uses a special algorithm to evaluate the degree of privacy impact of the requested query.

[*Step 3: Receive Query Result*] The differential privacy guard receives the response based on the undistorted data ([Step 3-2] in [Fig. 1]) by transmitting the query to the database containing various kinds of medical information, including personal information ([Step 3-1] in [Fig. 1]).

[*Step 4: Noisy Response*] The differential privacy guard adds an appropriate amount of noise due to the privacy effect. In other words, to protect the

confidentiality of the personal information in the database, it produces inaccurate results with noises added ([Step 4-1] in [Fig. 1]). And then it delivers the results to the analyst (See [Step 4-2] in [Fig. 1]).

Through the above process, the analyst can receive the result of applying noise that satisfies the differential privacy of the query that he/she has requested.

2. Problems of existing differential privacy methods using laplace noise[3]

R. Sarathy and K. Muralidhar[7] pointed out the problem of the Laplace noise method[8], which is one of the methods of implementing differential privacy, and proposed a solution to this problem. In the paper [7], the implementation of differential privacy using Laplace noise is based on the assumption that if the attacker knows all other data except one data (assuming that 49 different data out of 50 are known in the paper [7]), and in the worst case, the degree of privacy is lowered by $1/q$ per q-th query for each query, the problem that the differential privacy is not satisfied as the query is repeated is generated. For example, suppose a database has a total of 50 data. Let's say that one data that the attacker does not know is α, the remaining 49 data that are already known are β_i ($1 \leq i \leq 49$), and the noise value is y_i ($1 \leq i \leq 49$). The attacker requests the query of $\alpha+\beta_i$ using β_i and subtracts β_i from the query result as much as the number of i to obtain each $\alpha+y_i$ value (e.g. if i = 1, the query result is $\alpha+\beta_1+y_1$, and the attacker obtains $\alpha+ y_1$ by subtracting the value of β_1 from the resultant value), so that it is possible to estimate α using the averaging of the values.

This is a problem that occurs when the amount of noise obtained by substituting into the equation (1) for obtaining the Laplace noise value using a random number value between 0 and 1 is insignificant enough to be negligible (assume as μ =0, b=Δf/ε =1). Taking advantage of this problem, the attacker can estimate the information about the target that the attacker is aiming at.

$$X = \mu - bsgn(U)(1-2|U|) \quad (1)$$

As a solution to the above-mentioned problem, the solution presented in the paper [7] is that we

Table 1. Problem Example of The Laplace Noise

Subject	x	x_1+x_i	Random number	y_i	$R_i = (x_1+x_i)+y_i$	x_1 estimated value
1	***0.96302***					
2	0.04926	1.01228	0.09201	-1.69271	-0.68043	-0.72969
3	0.16718	1.1302	0.10861	-1.52684	-0.39664	-0.56382
4	0.24433	1.20735	0.77353	0.791996	1.999346	1.755016
5	0.54524	1.50826	0.90748	1.687183	3.195443	2.650203
6	0.30453	1.26755	0.04928	-2.31709	-1.04954	-1.35407
7	0.21408	1.1771	0.49193	-0.01627	1.160828	0.946748
8	0.45657	1.41959	0.68066	0.448352	1.867942	1.411372
9	0.31829	1.28131	0.88277	1.45047	2.73178	2.41349
10	0.1653	1.12832	0.85335	1.226559	2.354879	2.189579
11	0.73505	1.69807	0.90475	1.658103	3.356173	2.621123
12	0.48531	1.44833	0.09813	-1.62831	-0.17998	-0.66529
13	0.93479	1.89781	0.65985	0.385221	2.283031	1.348241
14	0.18673	1.14975	0.24145	-0.72795	0.421804	0.235074
15	0.23665	1.19967	0.96307	2.605584	3.805254	3.568604
16	0.38331	1.34633	0.9761	3.04073	4.38706	4.00375
17	0.7895	1.75252	0.00648	-4.34589	-2.59337	-3.38287
18	0.64746	1.61048	0.0219	-3.12812	-1.51764	-2.1651
19	0.51577	1.47879	0.76515	0.755661	2.234451	1.718681
20	0.44142	1.40444	0.04655	-2.37408	-0.96964	-1.41106
21	0.60352	1.56654	0.09416	-1.66961	-0.10307	-0.70659
22	0.07297	1.03599	0.97904	3.171992	4.207982	4.135012
23	0.78175	1.74477	0.21973	-0.82221	0.922561	0.140811
24	0.40297	1.36599	0.80222	0.927453	2.293443	1.890473
25	0.35075	1.31377	0.87472	1.384057	2.697827	2.347077
						0.933198

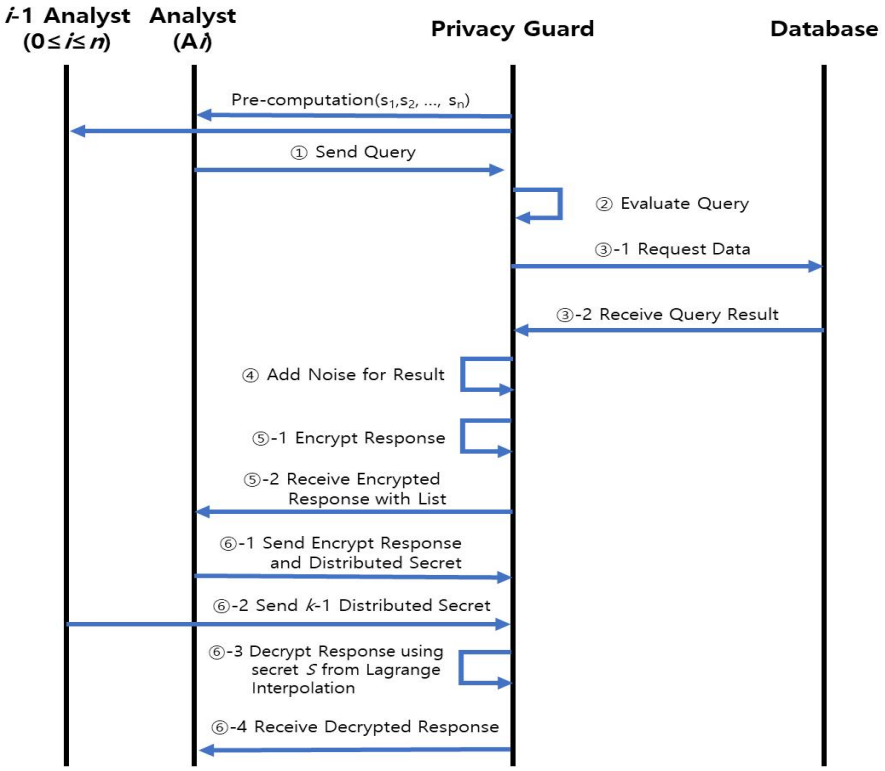

Fig. 2. The Previously Proposed Differential Privacy Process

propose a method to satisfy the differential privacy if the analyst (assuming a malicious attacker here) requests a series of queries, it applies q times noise to each q-th query by canceling the privacy, which is reduced by $1/q$ times for each q-th. The solution through this method is lowered in usability because the amount of noise is increased by q times so that too much noise is applied. In other words, we cannot actually utilize the value obtained from the result of the requested query. [Table 1] is an example made to show the problem described above. In [Table 1], x is an arbitrary real number between 0 and 1, y_i is a noise value generated according to a random number (arbitrary real number between 0 and 1), R_i is a value obtained by adding a noise value (y_i) to x_1+x_i and the estimated value of x_1 is a value obtained by performing $R_i - x_i$. In this case, it can be seen that the average value of the x_1 estimated values can be estimated as the approximate value of x_1 (that is, the average value 0.933198 of the x_1 estimated value column and the value 0.96302 of x_1 are similar values).

3. Problems of existing differential privacy method using secret sharing scheme[4]

The differential privacy method using the secret sharing scheme suggested by Shamir[9] solved the problem that the result of the averaging of the x_1 estimated values described in Section Ⅱ.2 can be estimated as the approximate value of x_1. The protocol for this technique is as follows (See [Fig. 2]).

[*Preliminary step: pre-computation*] In order to prevent conspiracy among various differential privacy analysts, n number of distributed secret information (referred as s_1, s_2, ... s_n) for the privacy guard and the shared secret key S among the analysts is generated using the (k, n) secret sharing technique and distributed to the n differential privacy analysts (referred to as A_1, A_2, ..., A_n).

[*Step 1: Send Query*] Analyst A_i asks the intermediary software called the differential privacy guard for a query.

[*Step 2: Evaluate Query*] The differential privacy guard uses a special algorithm to evaluate the degree of privacy impact of the requested query.

[Step 3: Receive Query Result] The differential

privacy guard receives the response based on the undistorted data ([Step 3-2] in [Fig. 2]) by transmitting the query to the database containing a variety of medical information, including personal information ([Step 3-1] in [Fig. 2]).

[*Step 4: Add Noise for Result*] The differential privacy guard adds an appropriate amount of noise according to the privacy effect on the result of the query received from the database. That is, it creates inaccurate results with added noise to protect the confidentiality of personal information in the database.

[*Step 5: Encrypt Response*] For the query requested by the analyst Ai, the noise-clipped result in [Step 4] is encrypted with a symmetric encryption algorithm such as AES[10] using the secret key S generated in the preliminary step ([Step 5-1] in [Fig. 2]). The differential privacy guard designates k-1 arbitrarily in n number of analysts who have the distributed secret generated in the [Preliminary step]. After that, the encrypted results are sent to the corresponding differential privacy analyst A_i who requested the query in [Step 1], along with a list of k-1 differential privacy analysts assigned ([Step 5-2] in Fig. 2).

[*Step 6: Decryption Response*] The analyst A_i who has received the result sends the encrypted result and his/her distributed secret to the privacy guard ([Step 6-1] in [Fig. 2]) and transmits the distributed secret of k-1 analysts corresponding to the list of differential privacy analysts specified in [Step 5] to the privacy guard ([Step 6-2] in [Fig. 2]). Then, the privacy guard calculates the secret information S using the Lagrange interpolation[5] and then decrypts the encrypted result using the symmetric encryption algorithm such as AES[10] ([Step 6-3] in [Fig. 2]). Then, the final result is sent to analyst Ai who has transmitted the encrypted result ([Step 6-4] in [Fig. 2]). At this time, the designation of k-1 differential privacy analysts except for the analyst A_i is arbitrary, but when the designation of k-1 is made to all n persons at least once, the secret key S generated by the privacy guard may be exposed to the differential privacy analysts, so the secret key S must be updated by performing the aforementioned preliminary steps again.

However, compared with the method proposed in Section Ⅱ.2, the proposed secret distribution technique[4] has the advantage of data usability and preventing conspiracy against the k persons, but because of the pre-distribution, the process of symmetric encryption and decryption, updating the shared secret key and the calculation process of finding the secret information S through the Lagrange interpolation method[5] are additionally incurred, the efficiency is deteriorated. In this paper, we try to solve this drawback by adding a 1-bit tag field, which is a status field, in the last column of a given dataset in the privacy guard's database to be able to know whether requested records by analysts were responded / given.

Ⅲ. The proposed Scheme

In this paper, we propose a method to add a 1-bit tag field, which is a status field, to the last column of a given dataset in the privacy guard database to solve the problems of the methods proposed in Sections Ⅱ.2 and Ⅱ.3. At this time, the tag field performs the role of checking whether or not there was a response (provision) of all m records, including individual patient medical information in the requested data set from the analysts. The problem with the method presented in Section Ⅱ.2 is that if the m-1 of record information among m records is provided to at least n of analysts, the remaining one piece of information can be found through conspiracy. Therefore, we would like to check whether up to m-2 records of the total m records are provided to the analysts through the tag field. If it is provided, we intend to prevent the conspiracy against analysts by updating the noise addition process (corresponding to [Step 4] in Section Ⅱ.3). This is because R. Sarathy and K. Muralidhar[7] have already demonstrated the problem in Section Ⅱ.2 when a maximum of m-1 records are provided. In

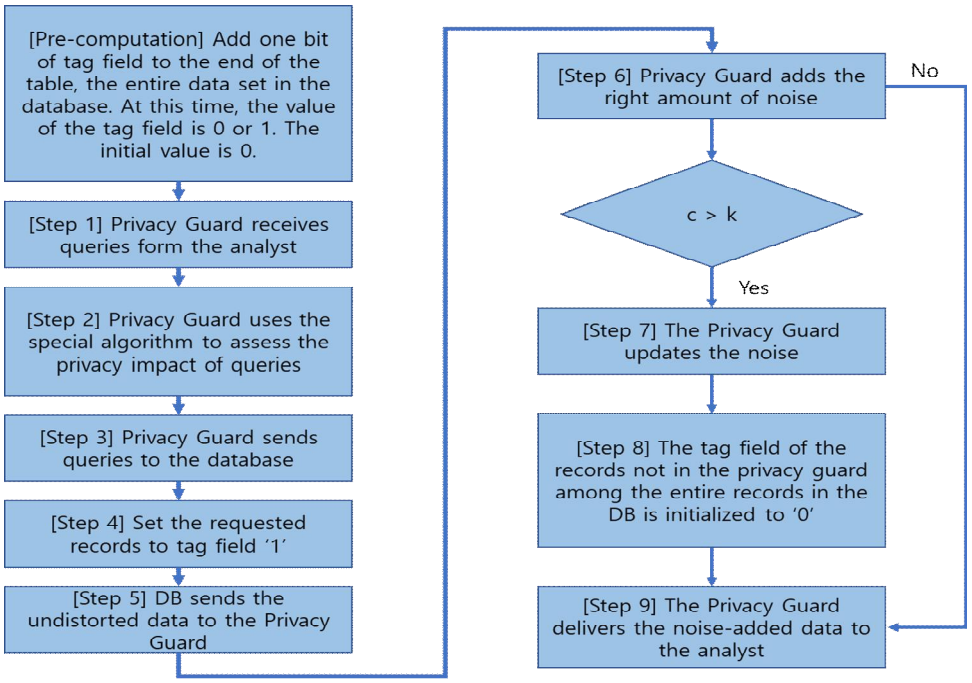

Fig. 3. Flow of The Proposed Scheme

fact, the privacy guard will be able to provide the analysts with records within a range of at least 1 to a maximum of m-2 of all m records. Of course, the smaller the number of records provided in terms of personal information protection, the safer it is. Therefore, it is left to the policy choice of the relevant institution about the number of records of the data set to be provided to the analyst by the privacy guard in this paper and it will not be discussed in this paper.

[Table 2], [Table 3] shows two examples of de-identifying data sets. At this time, Data set 2 is assumed to be the data requested to analyst *B* since Data set 1 was provided to analyst *A*. Data set 1 contains data for patients *A, C, D, E* and *F* and Data set 2 contains data for patients *A, B, C, G* and *H*. In the second requested Data set 2, the tag field of patients *A* and *C* has been changed to 1. At this time, if the value of the tag field is 1 among the entire records, it can be known that the record is requested by the analyst at least once.

The proposed method in this paper improves the differential privacy procedure[4] in Section Ⅱ.4 and the detailed procedure is as follows (see [Table 4] [Fig. 3] and [Fig. 4]).

Table 2. Examples of De-identification Data Set 1

Name	Sex	Code type	Code Format	Type of insurer	Tag
Patient A	2	11	021	4	0
Patient C	1	28	201	9	0
Patient D	1	81	071	4	1
Patient E	2	11	041	4	1
Patient F	2	11	131	7	0

Table 3. Examples of De-identification Data Set 2

Name	Sex	Code type	Code Format	Type of insurer	Tag
Patient A	2	11	021	4	1
Patient B	1	81	071	4	1
Patient C	1	28	201	9	1
Patient G	2	71	071	4	1
Patient H	2	61	061	5	0

Table 4. Notation

Acronyms	Contents
m	As the integer value, it is the total number of records in the dataset in the database and the initial value is zero.
k	As an integer value, the threshold value, the initial value is 0, used for determining whether to add a new noise or not is arbitrarily determined by the user within the range of minimum 1 to maximum *m*-2 according to the security policy.
c	As an integer value, it is the number of records with the tag field set to 1 out of all *m* records and the initial value is 0.

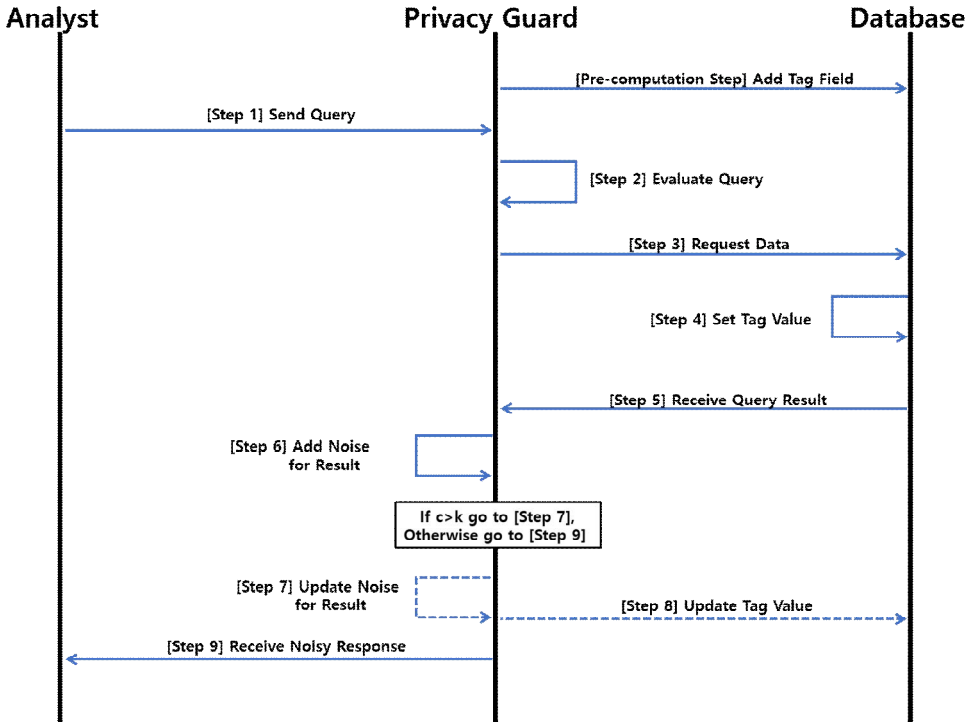

Fig. 4. The Proposed Scheme

[*Preliminary step*] Add the whole data set in the database, that is, the one-bit tag field that is the status field in the end column of the table. At this time, the value of the tag field is 0 or 1 and the initial value is 0.

[*Step 1: Send Query*] Analyst A_i asks the intermediary software called the differential privacy guard for a query.

[*Step 2: Evaluate Query*] The differential privacy guard uses a special algorithm to evaluate the degree of privacy impact of the requested query.

[*Step 3: Request Query Data*] The differential privacy guard transmits a query to a database containing a variety of medical information, including personal information.

[*Step 4: Set Tag*] Set the tag field value of all requested records (c) among all records (m) in the database to 1.

[*Step 5: Receive Query Result*] The database transmits a response based on undistorted data to the privacy guard.

[*Step 6: Add Noise for Result*] The differential privacy guard adds an appropriate amount of noise according to the privacy effect on the result of the query received from the database.

[*Step 7: Update Noise for Result*] If the value c is less than or equal to the predetermined threshold value k, this step is not performed and the process moves to [step 9] immediately. Otherwise, if the value c is greater than the value k, the differential privacy guard updates the noise because there is a risk of conspiracy between analysts.

[*Step 8: Update Tag Value*] Initialize the tag field stored in the database to 0, and update the tag fields to 1 for the currently requested records.

[*Step 9: Receive Noisy Response*] The differential privacy guard delivers the de-identifying data with added noise to the analyst.

1. Security analysis to the proposed scheme

[Table 5] compared privacy (safety), usability, preventing conspiracy and effectiveness (performance) in Dwork[3], R. Sarathy et al.[7], Kim et al.[4] and newly suggested method in this paper. First, in terms of privacy and the safety perspective of personal information, the method proposed by Dwork[3] and R. Sarathy et al.[7] basically uses differential privacy to ensure its safety. However, in

the case of the method proposed by Dwork[3], the problem described in Section Ⅱ.3 exists. In addition, Kim et al.[4] and the method proposed in this paper accept the method of Dwork[3] as it is, which basically satisfies differential privacy, and since the proposed method in this paper applies new noise periodically, the privacy is assured. Secondly, the proposed method of Dwork[3] in terms of usability perspective is superior in terms of usability because a small amount of noise due to Laplace noise is applied; however, there is also the same problem as described in Section Ⅱ.3. In addition, the method proposed by R. Sarathy et al.[7] uses a method of adjusting the amount of noise to improve the problem of Laplace noise. In this case, there is safety in that the amount of noise is greatly increased but because there is a big difference between the actual data, it is useless. However, unlike the method proposed by R. Sarathy et al.[7], the new method proposed in this paper updates the noise periodically according to the threshold k determined by the security policy of the hospital and each institution, so the safety is assured as well as the usability. Thirdly, the proposed method by Dwork[3] and R. Sarathy et al.[7] did not consider the conspiracy of analysts in terms of preventing conspiracy, but Kim et al.[4] is able to prevent the conspiracy by using the secret sharing technique as described in section Ⅱ.4. However, the method proposed in this paper can prevent the conspiracy because it cannot be utilized or compared with the previous data as the records of the data set in the whole DB update the new noise to the analysts when it exceeds the value k.

Finally, in terms of efficiency, unlike the method proposed by Dwork[3] and R. Sarathy et al.[7], there is some overhead in adding and verifying tags in each record in the data set, but it is considered to be negligible in terms of overall performance. For the method suggested by Kim et al.[4], as shown in [Table 6], because of the additional computation process to find out the secret information S through the pre-distribution by using the secret distribution technique, each process of symmetric encryption and decryption, each process of encryption and final output transmission, updating the shared secret key and the Lagrange interpolation[5] is added, the efficiency is deteriorated. However, the existing secret distribution technique is not used and the tag field is added to the last column of the given data set once, the tag update is performed twice when data is provided to the analyst, and the noise update is performed once to prevent conspiracy in the proposed method; therefore, it maintains the existing advantages and the efficiency is drastically improved.

Ⅳ. Conclusion and Future Works

Table 5. Security Comparison of The Proposed Scheme

	Dwork[3]	R.Sarathy et al.[7]	Kim et al.[4]	Suggested technique
Ensure privacy of personal information (safety)	△	O	O	O
Usability for actual data use	O	X	O	O
Preventing conspiracy	X	△	△	O
Efficiency (performance)	O	O	△	O

Table 6. Effective Comparison of The Proposed Scheme

	Previously proposed protocol	Newly proposed method
Preliminary step	Pre-distribution to the shared secret key S	Add tag to the last column of records in the DB
Step 4		Tag update once
Step 5	AES symmetric encryption once Encrypted result transmission once	
Step 6	Lagrange interpolation once AES symmetric decoding once Final result transmission once Update to shared secret key	
Step 7		Noise update once
Step 8		Tag update once
Number of transmissions	8 times	6 times

Large-scale medical information has many advantages for the development of the medical field and for the prevention of diseases. However, besides these advantages, large-scale medical information contains a lot of personal information, so there are many restrictions on its use. To overcome these drawbacks, various non-identification methods such as *k*-anonymity, *l*-diversity and differential privacy have been developed and utilized. In this paper, we have discussed the processing of differential privacy, the use of Laplace noise, and the problems mentioned by R. Sarathy et al.[7] and Kim et al.[4]. In addition, we proposed a new solution to update the noise by adding a one-bit tag field, which is a status field, to the last column of a given dataset and setting the threshold *k*. The proposed method theoretically proves to be better than the existing methods, not only in terms of privacy, but also in terms of preventing conspiracy and efficiency through [Table 5] and [Table 6].

We will prove the results through experiments for the proposed method in our future research.

REFERENCES

[1] L. Sweeney, "k-anonymity: a model for protecting privacy", Information : International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, Vol. 10, No. 5, pp. 557-570, 2002.

[2] Ashwin Machanavajjhala, Johannes Gerhrke, Daniel Kifer, "l-Diversity: Privacy Beyond k-Anonymity, Department of Computer Science", Information : Cornell University, 2007.

[3] Dwork, C, "Differential privacy" Information : In M. Bugliesi, B. Preneel, V. Sassone, and I.Wegener, eds., ICALP (2), Volume 4052, Lecture Notes in Computer Science, Springer, pp. 1-12, 2006.

[4] Cheoljung Kim, Kwangsoo Yeo and Soonseok Kim, "A New Differential Privacy Scheme Ensuring Security and Effectivenss", Information: An International Interdisciplinary Journal vol. 20, number 8(B), pp. 612-613 August 2017.

[5] Jean-Paul Berrut, Lloyd N, Trefethen "Barycentric Lagrange Interpolation" Information : SIAM Review, Vol. 46, No. 3, pp. 501-51, 2004.

[6] Microsoft Corporation, "Differential Privacy for Everyone", 2012.

[7] Rathindra Sarathy, Krish Muralidhar, "Evaluating Laplace Noise Addition to Satisfy Differential Privacy for Numeric Data", Information : Oklahoma State University - Stillwater, University of Oklahoma, April 2011.

[8] Aminta Stockute, Paul Johnson, "Laplace Distribution", June 10, 2013.

[9] Shamir Adi, "How to share a secret", Informationg : Communications of the ACM, Vol. 22, No. 11, pp. 612-613, November 1979.

[10] "Advanced Encryption Standard", NIST, Federal Information Processing Standards Publication 197, November 26, 2001.

Authors

Soon-Seok Kim received the M.S. and Ph.D. degrees in Computer Engineering from ChungAng University, Korea, in 1999 and 2003, respectively. Dr. Kim is currently a Professor in the Department of Computer Engineering, Halla University. He is interested in de-identification of personal information.