https://doi.org/10.33778/kcsa.2019.19.5.025

# Study on the New Re-identification Process of Health Information Applying ISO TS 25237

Soon Seok Kim*


## 요 약

With the development of information and communication technology, hospitals that electronically process and manage m edical information of patients are increasing. However, if medical information is processed electronically, there is still room for infringing personal information of the patient or medical staff. Accordingly, in 2017, the International Organization for Standardization (ISO) published ISO TS 25237 Health Information - Pseudonymization[1]. In this paper, we examine the re - identification process based on ISO TS 25237, the procedure and the problems of our proposed method. In addition, we p ropose a new processing scheme that adds a re-identification procedure to our secure differential privacy method [2] by ke eping a mapping table between de-identified data sets and original data as ciphertext. The proposed method has proved to satisfy the requirements of ISO TS 25237 trust service providers except for some policy matters.


# ISO TS 25237을 적용한 보건의료정보의 새로운 재식별 처리에 관한 연구

김 순 석*


## ABSTRACT

정보 통신 기술의 발달로 환자의 의료 정보를 전자적으로 처리하고 관리하는 병원이 증가하고 있다. 그러나 의료 정보가 전자적으로 처리되는 경우에도 환자 또는 의료진의 개인 정보를 침해 할 여지는 여전히 남아 있다. 이와 관련하여 2017년 국제 표준화기구 (ISO)는 ISO TS 25237 보건의료정보-가명[1]을 발표한 바 있다. 본 논문에서는 ISO TS 25237에서의 보건의료정보의 가명화 절차 및 제안된 방법의 문제점에 근거한 재식별 처리 과정을 검토하고자 한다. 또한, 우리는 비식별 데이터 세트와 원본 데이터 사이의 매핑 테이블을 암호문으로 유지함으로써 기본 우리가 제안한 바 있는 안전한 차등 개인 정보 보호 방법[2]에 재식별 절차를 추가하는 새로운 처리 방법을 제안하고자 한다. 제안하는 방법은 일부 정책적인 관리 문제를 제외하고는 ISO TS 25237 신뢰 서비스 제공 업체의 요구 사항을 충족시키는 것으로 입증되었다.


**Keywords : De-Identification, Differential Privacy, Medical Information, Privacy Protection, Re-Identification**

접수일(2019년 8월 11일), 게재확정일(2019년 9월 27일)

* 한라대학교 컴퓨터공학과

# 1. INTRODUCTION

Following the recent development in information technology, there has been an increase in the number of hospitals processing and managing their patients' medical information through electronic means. However, there still remains the possibility of the invasion of privacy for the patients or the medical staff. Accordingly, in 2017, the International Organization for Standardization (ISO) published ISO TS 25237 Health Information - Pseudonymization[1]. In this paper, we establish the basic definition of the process of re-identification and pseudonymization for the secondary use of private medical information, explain the irreversible and reversible pseudonymization, re-identification appraisal guide, the minimum requirement for re-identification, and other concepts. In particular, we suggest that re-identification may be demanded due to the following reasons: 1) To verify and prove the integrity of the data, 2) when there is request for additional data, 3) to notify the medical information provider or the agent of the private information of some important test results. Additionally, we discuss the method for processing such situations, and their technical realization.

In our previous paper [2], we have suggested a new protocol with better safety and efficiency than the differential privacy method which is a widely known de-identification technique. However, our protocol does not specify the procedure involving the re-identification process invoked by the aforesaid ISO TS 25237, and is subsequently flawed in that it is difficult to verify the integrity of the pseudonymized data and the original source data.

Accordingly, in this paper, we further expand the differential privacy method [2] employing a secret sharing scheme that we have provided in our previous paper and suggest a new method that abides by the re-identification procedure prescribed by ISO TS 25237.

In the second section of this paper we briefly discuss the re-identification process based on ISO 25237 as related research and proceed to find the weaknesses of differential privacy methods based on a secret sharing scheme that we have suggested before. In the third section, we suggest a new modified method that resolves such problems, and we end our paper on section four.

# 2. RELATED RESEARCHES

## 2.1 RE-IDENTIFICATION PROCESS BASED ON ISO 25237[1]

ISO 25237 is the international standard that includes the requirements and rules for pseudonymization for the de-identification of private information. There exists some cases in which de-identified information must be provided after being re-identified, and ISO 2537 states the following eight situations as such cases: to verify the integrity of the data, to verify and check copied data, to request additional data, when connected to a variable in additional research, to check the degree of compliance, to notify the medical information provider or the agent of the private information of some important test results, for further research, and for law enforcement.

### 2.1.1 RE-IDENTIFICATION PROCESS

The international standard re-identification process as prescribed by ISO 25237 can be divided into two cases: the process as a part of the standardized de-identification process, and an exceptional process of re-identification invoked in the case where an event has transpired.

Firstly, the standardized re-identification process refers to the re-identification process as a part of the entire process. If the re-identification process is a part of the standard process, the status and procedure of re-identification must be a part of the design as a whole. For example, a request for pseudonymization is sent from a medical record application program through an unidentified process. The result is accepted under a pseudonym, and automatically re-identified and recorded in the medical record by an application program. In a standardized process, re-identification must be carried out automatically and transparently, and no authorization should be required. If the re-identification process is a part of a standardized process, the integrity of the data should be assured in the following procedure. In such case, in most of the following procedure, the integrity of data can be requested and verified on the same level of private data. However, this is not necessarily the case for research data. In addition, the security of the set of data and control of private information must be taken into consideration for standard de-identified processes.

(FIGURE 1) depicts the process of de-identification as standardized by ISO 25237. Such process uses a sub-process including pseudonymization and anonymization. Such sub-processes utilize various tools in accordance with the type of data and the method for risk reduction.

Re-identification as an exceptional event is when a de-identified data requester requests re-identification under exceptional circumstances, and in such case the process requires a specific verification process and an exceptional intervention by a pseudonymization service provider. In such case where a de-identified data is re-identified, an exception from the rules must be considered, and the security policy must define such situations in which a re-identification process may be authorized. A security policy must further define estimated cases, and must meet the following criteria.

- The policy must explain the respective cases and must detail one or more re-identification scenario per case.
- Individuals who request re-identification must be identified.
- Requesters who object to the verification rules regarding re-identification must be identified. In such case, all participants must be fully aware of the re-identification event, and the re-identification must proceed only after the appropriate authorization (electronic or other) and must follow the scenario detailed in the policy.
- Re-identification must be carried out by a credible service provider. (Exceptional re-identification processing capabilities are required from the service provider.)
- It must be understood that circumstances that require control may transpire irrespective of the service provider, and all must be planned accordingly.
- The manager of the re-identified data must test for the integrity (accuracy, complete-ness) of the data.
- The policy must clearly specify who controls

personal data during the process of re-identification. This is because the identified data may not be as complete or as credible as the original personal data.

· The same rules as the rules for anticipatable circumstances should be applied under un-foreseeable and exceptional circumstances. This is because unforeseeable circumstances would most likely not have a re-identification scenario prepared for them. The gravity of the situa-tion regarding the request for re-identification must also be taken into account, and the responsibility falls under the data manager.

· Re-identification for the enforcement of law is an exception to the principles stated above.

### 2.1.2 REQUIREMENTS FOR THE TRUST SERVICE PROVIDER

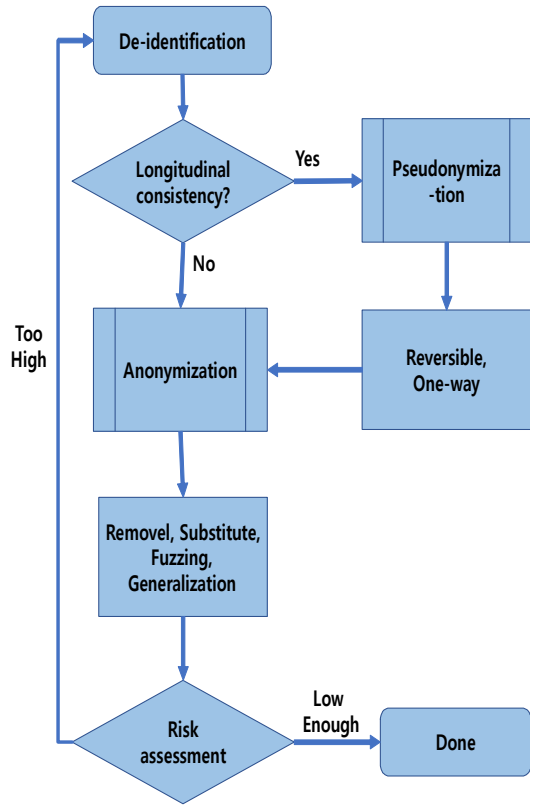
ISO 25237 states the following 17 requirements as requirements needed from trust service providers for re-identification and de-identification.

[Req. 1] The institution must be strictly autonomous from the original source provider.

[Req. 2] The management policy must be notified to the members to guarantee the safety and credibility of the used method.

[Req. 3] The security and credibility of the software module must be guaranteed, and the following requirements must be met. First, the module source and the integrity of the process must be warranted. Second, the integrity of the code must be vouched for using a code signature.

[Req. 4] The operating environment of the company and the security of its platform and infrastructure must be guaranteed, and the following requirements must be met. First, the net-work traffic must be limited to disallow any unnecessary traffic. Second, all unnecessary operation system services must not be used. Third, technological, physical, procedural and personnel management must be provided as prescribed by ISO 27799[3].




(FIGURE 1) The general de-identification process in the ISO 25237 standard

[Req. 5] A monitoring and quality assurance service and program must be realized for surveillance against malicious network infiltration and attacks, and for the quality assurance of the service.

[Req. 6] The encryption key must be managed under the supervision of multiple staff members, and the identifier must be encrypted and decrypted into two keys. One of the keys must be under the control of the

original data, and the other under the control of the pseudonymous service.

[Req. 7] The pseudonymous service must be documented, and the service must be recorded and be subject to inspection to prove the integrity of the service.

[Req. 8] The continuity of the pseudonymous service must be warranted through back up.

[Req. 9] Internal inspections must be documented and must be carried out at least once a month.

[Req. 10] The requirements for external inspections are as follows: one, it must be carried out by a trusted institution that follows a publicized operational procedure and meets a set degree of customer satisfaction. Two, the inspector must be under a separate institution from the pseudonymization service provider. Three, the inspector must have no financial interest in the organization being inspected. Four, the inspector must have the authority necessary to inspect an information system to a necessary degree. Five, the service provider must immediately notify any faults in the pseudonymization service found during the inspection.

[Req. 11] Requirements for the participants are as follows: one, the organizational keys related to pseudonymization must maintain their integrity. Two, the related systems must be under physical, personal, and technological control as prescribed by ISO 27799[3]. Three, the participants are responsible for the protection of the private information including the pseudonymized information resources, and for the pseudonymization of the payload data.

[Req. 12] Risk assessments must be carried out in relation to the original data of the pseudonymized result data, and such restrictions must be stated in the management policy.

[Req. 13] The pseudonymization service provider should only carry out re-identification for data sets drawn from an original source.

[Req. 14] The data controller is responsible for the re-identification of patients.

[Req. 15] The environmental and legal restrictions regarding the deactivation of the re-identification key and the security devices must be notified to support the level of personal information protection required from the service.

[Req. 16] The quality and availability of the service must be specified and must be provided if requested.

[Req. 17] Some unnecessary identifiers may become clouded or covered.

## 2.2 DIFFERENTIAL PRIVACY METHOD EMPLOYING A SECRET SHARING TECHNIQUE[2]

In our previous paper [2], we have suggested a new protocol with improved security and efficiency based on the well-known differential privacy technique[4]. The following summarizes the suggested protocol with the number of analysts assumed as $n$ (refer to (FIGURE 2)).

[*Pre-computation*] To prevent collusion among the differential privacy analysts, the privacy guard employs a ($k$, $n$) secret sharing scheme[5, 6] and creates a total of $n$ shared secrets ($s_1$, $s_2$, …, $s_n$) regarding the secret key $S$ shared among the privacy guard and the analysts and distributes it among the n differential privacy analysts ($A_1$, $A_2$, …, $A_n$).

[*Step 1 : Send Query*] Analyst $A_i$ requests query to the middle software known as the privacy guard.

[*Step 2 : Evaluate Query*] The differential privacy guard uses a special algorithm to assess projected affect of the query on privacy.

[*Step 3-1 : Request Query Data*] The differential privacy guard sends the query to the database containing information of medical treatment including private information.

[*Step 3-2-1 : Input file / Apply Cache in Map Process*] The original input file is too big to be processed in a single step and a process in which the data is chunked into manageable size(64MB for Hadoop models for example[7]) must be carried out. Special attention and care must be paid to the fact that the chunked files are too small, the segmentation, management, and map task generation can cause overhead. Before the appropriately chunked files are sent to the next stage, the cache hit must be checked During this process, hit data are immediately processed to [Step 3-2-2] and other data remain in the cache for the next hit.

[*Step 3-2-2 : Map, Combine, Partition*] During the map process, the data is read and divided into keys and values. During the next process, the combining process, the key values are used as a standard for combining data. The reason why such process is included in the map process despite the fact that the reduce function carries out the same process is because the map function is executed in the local system while the reduce function uses a network to transfer information, and the combine process reduces the amount of data transferred through the network. In the next step, the partition process, the combined value is stored in separate partitions. The partitions are divided in accordance with the value of the key.

[*Step 3-3-1 : Apply Cache in Reduce Process*] Before the reducer process is carried out on the final data, the cache must be applied once again, and if there is a hit the data should be processed immediately to [Step 3-3(2)]. Other data must remain in the cache for the next hit.

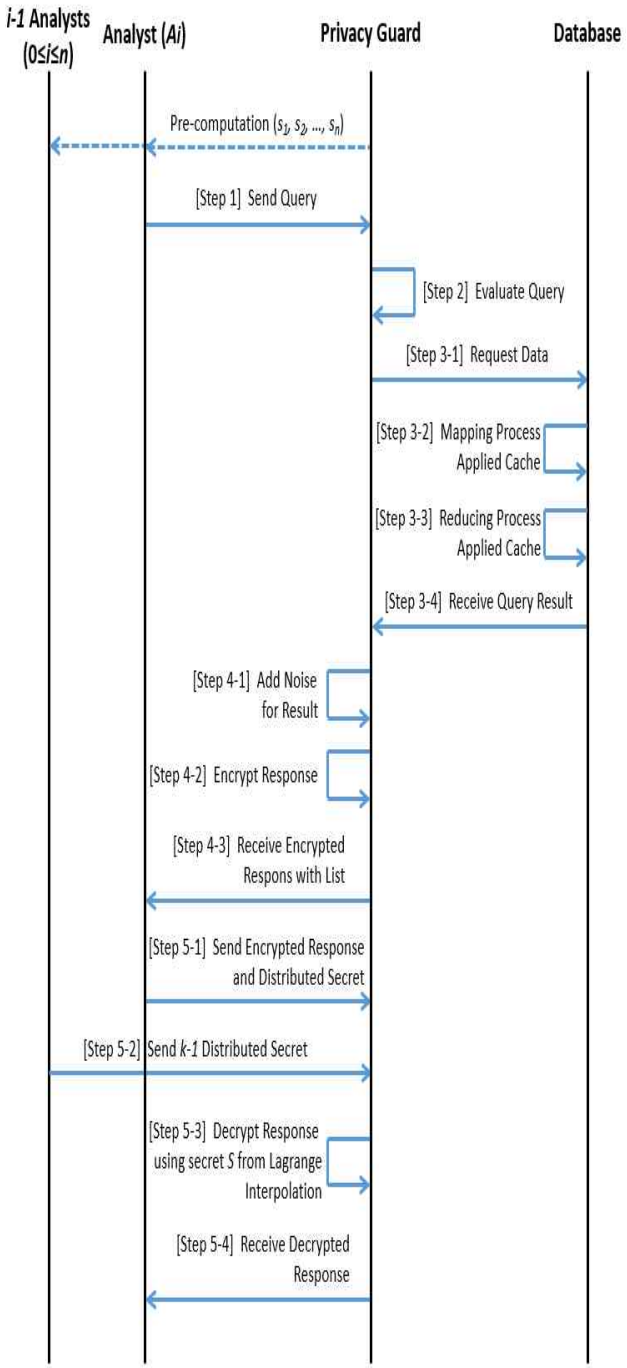
[*Step 3-3-2 : Shuffle, Sort, Reduce*] After the shuffling process is carried out to combine the results of the map function and to transfer the data to the reducer, the sorting process is carried out to divide the result data according to their key value. And finally the reduce function similar to the combine function in which the data is combined according to their key value is carried out.

[*Step 3-4 : Receive Query Result*] A response based on de-distorted is received from the database through [Step 3-2, 3-3].

[*Step 4-1 : Add Noise for Result and Encrypt*] The privacy guard adds an appropriate amount of noise according to the result they received from the database. In other words, the noise added to protect the privacy of personal information creates an inaccurate result.

[*Step 4-2 : Encrypt Response*] The noise-added result is encrypted by a symmetric code algorithm like AES[8] using the secret key $S$ generated in the prior stages.

[*Step 4-3 : Receive Encrypted Response with List*] The differential privacy guard selects a total of $k-1$ analysts from the $n$ analysts who possess the shared secret generated from [Pre-computation]. Afterwards,




(FIGURE 2) Differential privacy procedure using secret sharing

the list of the designated *k-1* differential privacy analysts is sent to differential privacy analysts $A_i$ along with the encrypted result from [Step 1].

[*Step 5-1 : Decrypt Response*] Analyst $A_i$, after receiving the result, sends the encrypted result to the privacy guard along with his own shared secret.

[*Step 5-2 : Send Encrypted Response and shared secret*] The *k-1* differential privacy analysts who were designated in [Step 4] send their shared secret to the privacy guard.

[*Step 5-3 : Decrypt Response Using Secret S from Lagrange Interpolation*] The privacy guard uses Lagrange interpolation to calculate the secret information $S$ and to decipher the encrypted result using a symmetric code algorithm such as AES[8].

[*Step 5-4 : Receive Decrypted Response*] The encrypted version of the final result is sent to analyst $A_i$. All differential analysts with the exception of $A_i$ must be designated randomly. However, if all n people in the pool have been designated as one of the *k-1* differential analysts, a new secret key S must be generated following the procedure described above as the secret key $S$ generated by the privacy guard may be in danger of being exposed to the differential privacy analysts.

During the above procedure, the queries requested and result data received through $A_i$ is not be documented. Consequently, there is no means to comply to any requests to check the integrity of the original data and the copied data, or any requests for re-identification for the purpose of verifying the record of the copied data or for the creation of additional data. However, in the method we suggest in this paper, we have added a mapping table that is able to connect

the de-identified data with the source data which is encrypted and stored to allow the function of re-identification.

## 3. THE PROPOSED RE-IDENTIFICATION METHOD

In section 2.2, in relation to solving the re-identification problem of the differential privacy method using the secret sharing scheme[5, 6], we suggest an idea that is basically to maintain an encrypted mapping table for the original data set and the provided data set. In case of a request for re-identification by a verified user, we create a process in which the encrypted code is deciphered and the source data and the de-identified data are reconnected to send the requested data to an analyst, thereby abiding by the international standard of ISO 25237.

In this paper, in relation to the service policy, we assume that requirements 1), 2), 3), 4), 5), 6), 8), 9), 10), 11), 12), 15), 16) for trust service providers listed in 2.1.2 are met.

In <TABLE 1>, <TABLE 2>, <TABLE 3> below, we provide an example mapping table using two data sets: Data set 1 and Data set 2. We assume that Data set 1 is the de-identified data already provided to analyst A, and Data set 2 is the original data of Data set 1. Data set 1 and 2 has the information for 5 patients, and in the mapping table are the original data for patient ID and the de-identified patient ID field. For example, if the clinical subject ID field 'AA34042' of the mapping table is connected to patient A via patient A's pseudonym identifier which allows the pseudonymized entity 'AA34042' to be re-identified as patient A. Therefore, if there is any request for re-identification, such mapping table can provide such service by utilizing the mapping table to refer to the original Data set 2 by referring to Data set 1.

The method we suggest in this paper adapts to the rule prescribed by ISO 25237 by improving the differential privacy method described in section 2.2, and the detailed process is shown below. (refer to (FIGURE 3)).

In the protocol suggested in (FIGURE 3), we assume that the data set for a specific patient has been requested from analyst $A_i$, and has already been provided. Refer to section 2.2 of our previous paper [2] for details.

<TABLE 1> EXAMPLE OF NON-IDENTIFICATION DATASET (DATASET 1)

| Clinical subject ID | Clinical trial ID | Regional Code | Gender Code | Age |
|---|---|---|---|---|
| AA34042 | BA0612 | 33 | 1 | 76~80 |
| AA20512 | GE1634 | 62 | 9 | 71~73 |
| AA93117 | GR8345 | 51 | 2 | 91~95 |
| AA03916 | NF7423 | 23 | 2 | 56~60 |
| AA11335 | BA0612 | 33 | 1 | 81~85 |

<TABLE 2> EXAMPLE OF SOURCE DATASET (DATASET 2)

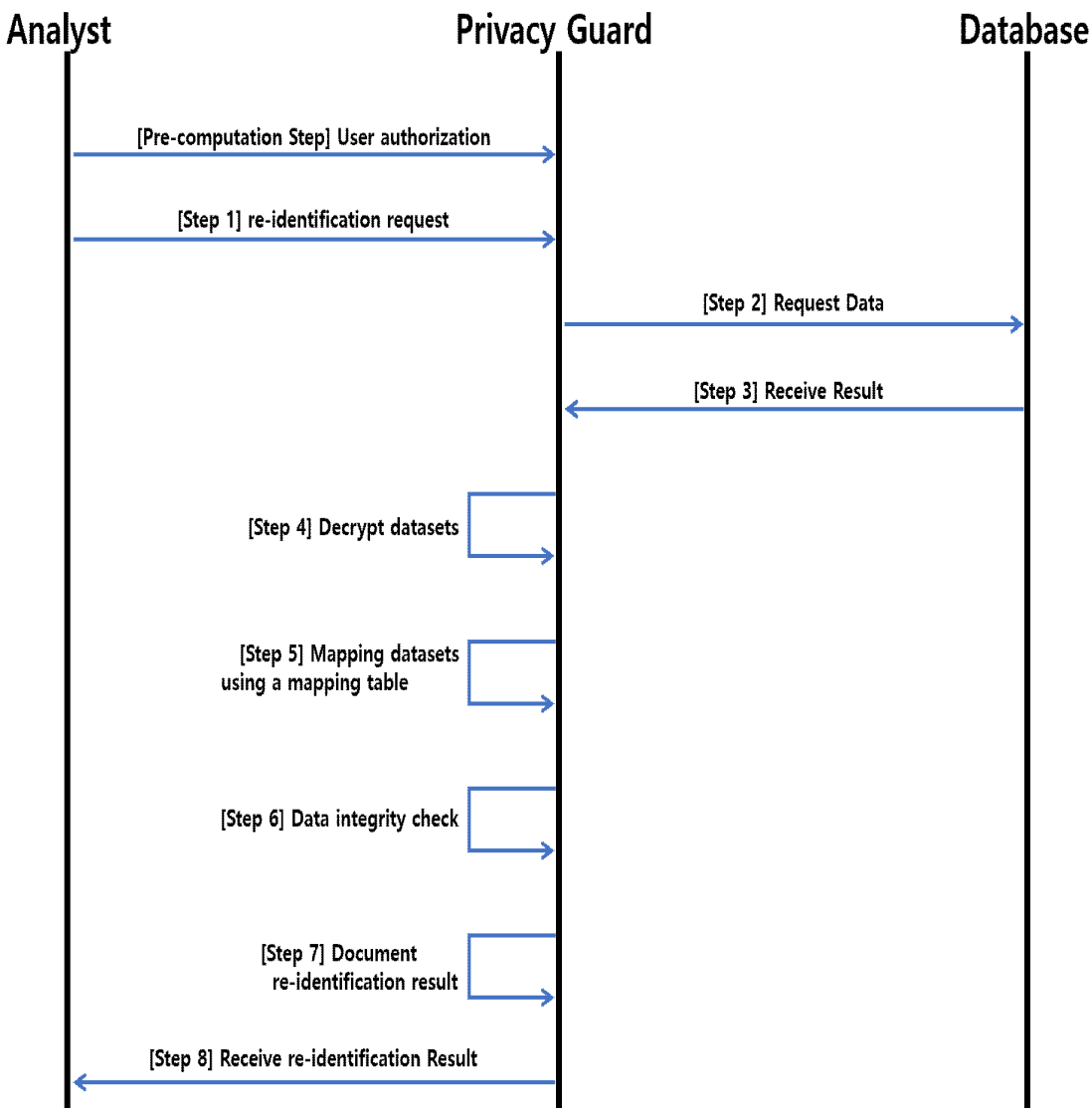
| Patient ID | Clinic ID | Region | Gender | Age |
|---|---|---|---|---|
| Patient A | B015 | Seoul | Male | 77 |
| Patient B | P113 | Busan | Other | 73 |
| Patient C | A588 | Gangwon | Female | 95 |
| Patient D | X395 | Gyeonggi | Female | 58 |
| Patient E | B015 | Seoul | Male | 82 |

<TABLE 3> EXAMPLE OF MAPPING TABLE

| Patient ID | Clinical subject ID |
|---|---|
| Patient A | AA34042 |
| Patient B | AA20512 |
| Patient C | AA93117 |
| Patient D | AA03916 |
| Patient E | AA11335 |

We also suggest the following additional processes to be carried out prior to starting the re-identification service for analysts.

[*Pre-computation : User authorization*] Analyst $A_l$ uses the middle software called differential privacy guard to verify the user. Electronic authentication should be carried out using the authentication certificate x.503.v3, which is based on a public key structure. A




(FIGURE 3) The process of proposed method

mapping table consisting of two fields, the original data set(refer to section 2.2.), and its de-identified version, and the actual patient ID field, and the de-identified patient ID field, should be encrypted and stored respectively. It is assumed that a bidirectional international standard symmetric code (Such as AES) is used for the encryption, as it must be deciphered later when requested by the analysts. If actual patient ID or clinical subject ID are pseudonymized, a unidirectional method such as hashing, pseudo random generator, or logical bit string functions can be used. Encryption or deciphering algorithm used in such cases are subject to the choice of the user and is not discussed in this paper.

[*Step 1 : re-identification request*] Analyst $A_i$ requests an additional re-identification to the differential privacy guard on a specific data set which has already been requested prior to the re-identification (e.g. additional attribute data for specific patients whose data has already been requested for additional research purposes). It is assumed that this re-identification process is an exceptional case (refer to section 2.1.1).

[*Step 2 : Request Data*] The differential privacy guard assesses the necessity of the data requested from analyst $A_i$. If they are deemed as necessary, it requests to the database the original data, de-identified data, their mapping table, and the cryptogram for the specific data set. If they are deemed unnecessary, the stage is terminated and the analyst is notified that the service is unavailable.

[*Step 3 : Receive Result*] The database sends the three cryptograms to the privacy guard.

[*Step 4 : Decrypt datasets*] The differential privacy guard deciphers the three cryptograms it has received from the database.

[*Step 5 : Mapping datasets using a mapping table*] The differential privacy guard uses the mapping table to connect the original data and de-identified data that had been decrypted in [Step 4].

[*Step 6 : Data integrity check*] The differential privacy guard uses cryptologic hashing function to carry out an integrity test for the original data and de-identified data.

[*Step 7 : Document re-identification result*] The differential privacy guard encrypts the re-identified data per the request of analyst $A_i$ and documents it and stores it along with the encrypted data. Identifiers are masked if they are assessed to be unnecessary during the re-identification process. The document should include the individual whose personal information has been revealed, time and date of re-identification, and the purpose of the re-identification, and more.

[*Step 8 : Receive re-identification result*] The differential privacy guard uses the authentication certificate x.503.v3[9], which is based on a public key structure, to safely transfer the result of the re-identification to the analyst.

## 3.1 ANALYSIS OF THE SUGGESTED METHOD

The basic security of the method we have suggested is connected to the security of the public key structure of authentication certificate x.503.v3[9], and the cryptologic primitives in relation to the mapping table, the original data, and the de-identified data.

In this section, we discuss whether the protocol we have suggested meets all of the requirements for trust service providers prescribed by ISO 25237 as mentioned in section 2.1.2. However, as we have stated before, we do not discuss requirements 1), 2), 3), 4), 5), 6), 8), 9), 10), 11), 12), 15), 16) as they are more related to service policies.

<TABLE 4> ANALYSIS OF THE REQUIREMENTS OF THE PROPOSED METHOD

| Requirement | Fulfilled | Details |
|---|---|---|
| Req. 7 | O | The re-identified data is recorded and stored in [Step 7]. |
| Req. 13 | O | Only the specific data set requested by analyst $A_i$ is requested to the database by the privacy guard in [Step 2]. |
| Req. 14 | O | The privacy guard controls the entire process of re-identification. |
| Req. 17 | O | In [Step 2] the necessity of providing the data is assessed, and in [Step 7], if certain identifiers are assessed as unnecessary, they are marked. |

<TABLE 4> indicates how the method suggested in this paper meets the requirements for trust service providers as prescribed by ISO 25237. Firstly, for [Req. 7], the method suggested in this paper (refer to (FIGURE 3)) meets the criteria, as the re-identification process is documented and stored in [Step 7]. [Req. 13] is met as only the specific data sets requested by analyst $A_i$, and not the entire data sets, are re-identified in [Step 2]. [Req. 14] is met as the privacy guard controls the entire process of re-identification. [Req. 17] is met as in [Step 2], the necessity for providing the data is assessed, and in [Step 7], any identifiers that are deemed unnecessary during the process of re-identification are masked. Therefore, the method we have suggested in this paper meets all of the requirements for trust service providers as prescribed by ISO 25237 with the exception of requirements regarding the service policy.

# 4. CONCLUSION AND FUTURE RESEARCH DIRECTION

Following the recent development in information technology, there has been an increase in the number of hospitals processing and managing their patients' medical information through electronic means. However, there still remains the possibility for the invasion of personal information of the patients or the medical staff if medical information is processed electronically. Accordingly, in 2017, the International Organization for Standardization (ISO) published ISO TS 25237 Health Information - Pseudonymization[1]. In this paper we have discussed the re-identification process based on ISO 25237, and the problems for the method we had previously suggested [2]. We have also suggested a new re-identification scheme that preserves an encrypted mapping table between the de-identified data set and the original data set, which adds to the re-identification process of our previous differential privacy method[2]. We have also shown through <TABLE 4> that our new method meets all of the requirements for trust service providers prescribed by ISO 25237.

In the future research, we aim to conduct an experiment to prove the result of our suggested method.

## REFERENCES


[1] ISO 25237, "Health informatics - Pseudonymization", 2017, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:25237:ed-1:v1:en

[2] 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. 6137-6147 August 2017.

[3] ISO 27799, "Health informatics - Information security management in health using ISO/IEC 27002", 2016, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:62777:en

[4] C. Dwork and G. N. Rothblum. "Concentrated differential privacy" CoRR, abs/1603.01887, 2016.

[5] Shamir Adi. "How to share a secret", Communications of the ACM. November" vol. 22, no. 11, pp. 612-613, 1979.

[6] Blakley G. R. "Safeguarding cryptographic keys", Proceedings of the National Computer Conference, vol. 48, pp. 313-317, 1979.

[7] J. Dean and S. "Ghemawat, MapReduce: simplified data processing on large clusters", Communications of the ACM - 50th anniversary issue: 1958 - 2008, vol. 51, issue 1, pp. 107-113. 2008.

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

[9] Housley R, Polk W, Ford W, and D. Solo, "Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[10] ISO/IEC 18033-3:2010, "Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers Health informatics". 2010, [Online]. Available: https://www.iso.org/obp/ui/#!iso:std:54531:en

[11] Jeong-mo Yang, "A Study on primitive p olynomial in stream cipher", Convergence Security Journal, vol. 18, no. 4, 2018

[12] Jong-ho Noh and Hun-yeong Kwon, "A Study on smart energy's privacy policy", Convergence Security Journal, vol. 18, no. 2, 2018

[13] Young-sook Lee, "Security Enhancement to an Biometric Authentication Protocol f or WSN Environment ", Convergence Sec urity Journal, vol. 16, no. 6, 2016


## 〔저자소개〕


김 순 석 (Soon-Seok Kim)
2003년 3월 ~ 현재 원주 한라대학교 컴퓨터공학과 부교수
2003년 2월 중앙대학교 대학원 컴퓨터공학과 박사
관심분야 : 개인정보 비식별, 암호응용
email : sskim@halla.c.kr