# New Secret Sharing Scheme for Privacy Data Management

You-Jin Song*, Dong-Hyeok Lee*

*Dongguk University.

**Abstract**

In ubiquitous environment, private enterprise or public institution's privacy data are sometimes exposed to hackers because of the lack of the sense of information security. We apply secret sharing scheme to solve the privacy problems. But, the existing secret sharing scheme are not suitable for the management of large a quantity of data because that required operation of large capacity. In this paper, We propose new secret sharing scheme for privacy data management. Our scheme makes high-speed operation possible, and it also allows for set weight for each secret pieces depending on weight of participants. The scheme proposed in this paper makes it efficient to collect and manage secure privacy data in ubiquitous environment.

## I. Introduction

Ubiquitous computing is recognized as a new business paradigm. Enterprises collect and manage privacy data for business activation. The technology which is appropriate for privacy data management is needed.

Recently, Customer Relationship Management(CRM) has been a requirement for strengthening competition of enterprise. It increases in collecting and managing privacy data.
But, private enterprise or public institution's privacy data are sometimes exposed to hackers because of the lack of the sense of information security.

For example, a malicious attacker might collect the user's information illegally such as the purchasing pattern, and the price of products etc. In this case, the attacker can use these data improperly at black marketing.

In the last few years, the recent marketing paradigm is shifted to database marketing from mass marketing. Database marketing provides service with consumers by recognizing them as individuals rather than groups. Therefore, maybe consumers feel more convenient through customized service.

Enterprises collect detailed privacy data and utilize them for efficient operation of database marketing in a various way.
But, privacy data is essential in DB marketing. It is possible that many privacy data , activity and sensitivity data stored in database of enterprise.

This case causes problems about the invasion of user's privacy.

On the other hand, if customers are given the authority to control a person's private information, enterprises can be overloaded.
In the meantime, it is possible that local administrator can still acquire privacy data from enterprise's database.
The administrators who have an access to private information may collect privacy data in an illegal method.
In this case, if the local administrator send illegally collected information to malicious attackers by e-mail or in the other way, It might bring about huge damage to user's privacy.
Therefore, new data management techniques for privacy protection is needed.

We apply secret sharing scheme to solve the problems mentioned above.
Secret Sharing scheme is a secure management protocol by splitting original data into several secret pieces. And the participants who have an access to private information are able to reconstructs original data through special operation.

## II. Comments on Traditional Secret Sharing Scheme and Contributions of this Paper

Secret sharing scheme is a technology that deals with secret pieces assigned to participants and when necessary, can reconstruct them by collecting part of pieces.

Representative secret sharing scheme is threshold secret sharing scheme that has been proposed in 1979[5].
But, this scheme is a static access structure and there is a limitation. I.e., a new secret sharing scheme for privacy data management is required.

### 2.1 Practical Problems for Handling Privacy Data

The traditionally proposed secret sharing scheme requires big-sized memory in operation. Therefore, it is not suitable for a large quantity of data management that is stored in ISP(Information Service Provider), etc.

For example, Shamir's threshold Scheme can't reuse information of participants after reconstruction and secret size is limited in exponent q of a prime number.
Also, as q increases, the size of secrets goes up at an exponential rate because it has limitation to management of large quantity data.

On the other hand, dealers can create polynomial expression and re-distribute new shares secretly to the current participants depending on change of access structure. These cases are not suitable for dynamic access environments that provide data in terms of lawful request of personal information.

Cachin proposed online secret sharing scheme in 1995. His scheme can provide the capability of sharing multiple secrets and to dynamically add participants on-line for general access structure, but it required a distributed computation for each shares[6].

To supplement this, the online multiple secret sharing schemes based on Diffie-Hellman and one-way function are proposed by Pinch[4] and Godoshi[3], but their scheme can't apply to management of privacy data because it

has a problem of the requirement of large capacity calculation due to modulo exponent operation.

Our scheme can be used to collect and manage privacy data because it supports simple and rapid reconstruction that is multiplication and addition operation each of k times.

2.2 Traditional scheme does not considered for character of privacy data

Unspecified persons or several storage can share secrets by using secret sharing scheme, and it can apply to secret data that are stored.

The traditional scheme does not have special problems with storing secret data except from operation speed problem.
But, the case of providing for personal information, information owner should determine how much, and to whom the privacy data had to be opened. Also, it requires structures that can designate weight of competence according to participant's importance.

This problem can be solved by the application of weight to secret sharing scheme.
After deciding weight to each secret piece that contains personal information, the administrator has an access to private information (in charge of information security) should reconstruct original data by collecting several secret pieces.
The method that is intended for designation of open ratio for privacy data is secret pieces which have each other weight according to grade or duty. In this paper, we can determine open ratio of privacy data through w-table.

The w-table is similar to the key that is used in encryption, but decisively, there is difference that is illustrated so below :
- Simply collecting w-table doesn't work for the attackers.
- Must collect data more than specific quantity for original data reconstruction.
- w-table is handled separately, and need not to consider security specially.

## III. The Proposed Scheme

The new secret sharing scheme that is proposed in this paper is as follows.

3.1. Notations

Notations that is used in this section is as following.

**W**(Weight) - Degree of data opening. i.e., weight of secret pieces.
**w-table** - Set of all weight
**O**(Original data) - Original Data
**L** - Set of secret pieces
**nid**(Number ID) - Serial number of each secret pieces.
**k** - Collected secret pieces for reconstruction.
**b** - Number of buffers
**bid** - Serial number of each buffers. ($B_{bid}$ : The Buffer B that has nid)
S - Secret Piece ($S_{nid}$ : The Secret Piece S that has nid)
**n** - Number of spllited secret piece

3.2. Preliminaries

A secret sharing scheme is a protocol between a set of participants $P = \{P_1,...P_n\}$ and a dealer D, where $D \notin P$ is assumed. The access structure $\Gamma \subseteq 2^P$ is a family of subsets of $\{P_1,...P_n\}$ containing the sets of participants

qualified to recover the secret.
It is natural to require Γ to be monotone, that is, if X'⊄Γ and X⊆X'⊆P, then X'∈Γ. A minimal qualied subset Y∈Γ is a set of participants such that Y'∈Γ
for all Y⊂Y, Y'≠Y. The basis of Γ, denoted by Γ0 , is the family of all minimal qualified subsets.

A computationally secure secret sharing scheme K is a protocol between D and the members of P to share a secret K, respective to an access structure Γ such that
a) the dealer D transmits a share Si secretly to participant Pi, for i=1,,,n,
b) all qualified sets of participants X∈Γ can efficiently compute K from their set of shares {Si|Pi∈X}, and
c) every unqualified subset of participants X ⊄Γ running any polynomial-time.

One way function on G, $f : G \rightarrow G$ such that $f(x)$ is easy to compute for all $x \in G$ (i.e. can be computed in time polynomial) and that it is computationally infeasible, for a given , to find an $x \in G$, to find an $x \in G$ such that $f(x)=y$. This notion can be made rigorous analogous to the definition of security[1].

3.3 Secret Splitting Scheme
Original data can be split by simple operations.
For splitting, decide the original data and the number of secret pieces and w-table.
After then, convert the original data to binary number and set threshold value and buffer size.
We can get a set of secret pieces which are constructed from the threshold value. The set met with threshold value is equal to original data.
Secret splitting scheme is shown as Fig.a.

Input : O, n, W(w-table)
Output : L = {S1, .. , Sn}
Assume : Lk = O
Step 1 : Convert original data to binary data.
o ← (O)2,
Step 2 : Set Threshold value and buffer size

$$t \leftarrow \frac{b}{2} + 1, \quad b \leftarrow \sum_{nid=1}^{n} W_{nid}$$

Step 3 : Let number of t be equal to original, and the other is different.

$$\forall_{d=1}^{b} S_d = \begin{cases} O & \text{if } 1 \le d \le t \\ O^{-1} & otherwise \end{cases}$$

Step 4 : Get L by collecting a set of buffers that have a nid with 1 to n.
L = {S1, .. , Sn}

Fig.a. Secret splitting scheme

3.4 Secret reconstruction scheme
The Secret reconstruction scheme is much simpler than splitting scheme.
By secret reconstruction scheme, we can reconstruct original data safely through set of collected secret pieces and w-table. The original data is reconstructed by multiply element by weight and compare to $\frac{b}{2}$.

**Input** : Set of collected secret pieces (Lk) , W
**Output** : Original data(O)

**Step 1** : Calculate buffer size for reconstruction.

$b \leftarrow \sum_{nid=1}^{k} W_{nid}$

**Step 2** : Get original binary data by multiplying element by weight and compare to $\frac{b}{2}$.

$$o = \begin{cases} 1 \text{ if } \frac{b}{2} \leq \sum_{nid=1}^{k} W_{nid} S_{nid} \\ 0 \text{ otherwise} \end{cases}$$

**Step 3** : Reconstruct to convert binary data to decimal data.

$O \leftarrow (o)_{10}$

Fig.b. secret reconstruction scheme

## IV. Example

In this section, we will give specific examples of new secret sharing scheme.

4.1 Motivation Scenario

Suppose Bob's credit card PIN number is 7342.

Bob does not want his PIN number to be known by anyone, and the PIN number is very sensitive secret information.

In this section, we will verify our scheme through splitting and reconstruction of secret pieces about Bob's credit card PIN number.

4.2 Data Splitting scenario

Input : Bob wants to split secret information about his credit card PIN number into five pieces. And every secret piece has nid and weight such as Table a. Weights consists of positive number, and Bob records w-table.

Table a. Weight for secret pieces

| Description | nid | Weight |
|---|---|---|
| Secret Piece A | 1 | 3 |
| Secret Piece B | 2 | 2 |
| Secret Piece C | 3 | 1 |
| Secret Piece D | 4 | 1 |
| Secret Piece E | 5 | 1 |

**Step 1** : Bob calculates binary number from 7342 that is taken to be original data.

i.e., 1110010101110 is created from 7342.

**Step 2** : Set buffer size according to w-table and calculate threshold value.

Buffer size can be calculated as following, and buffer created as Fig.c.

$$b = \sum_{nid=1}^{n} W_{nid} = 3+2+1+1+1 = 8$$

| buffer | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 |
|---|---|---|---|---|---|---|---|---|
| $S_{nid}$ | S1 | S1 | S1 | S2 | S2 | S3 | S4 | S5 |

Fig.c. Created buffer for secret splitting

Threshold value can be calculated as following :

$$t = \frac{b}{2} + 1 = \frac{8}{2} + 1 = 5$$

**Step 3** : Input data to buffer.

The description of the input data is as following :

In Step 2, Make buffers of 8 numbers and threshold value set by 5 for secret sharing.

Here, t, i.e., buffers of 5 have the data that is equal to the original one, and other buffers have data that is different from the original.

For example, look into splitted sequence number 1 from Fig. d, we can see five numbers of 1 and three numbers of 0 by splitting bit sequence converted from binary number.

The data is placed randomly and buffers that

have the same nid should have an identical number of bit 1.

Fig.d. shows splitted data.

| Source | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Splitting

| Bbid | Snid | Splitted Sequence Number | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| B1 | S1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| B2 | S1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| B3 | S1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| B4 | S2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| B5 | S2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| B6 | S3 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| B7 | S4 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| B8 | S5 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |

Fig.d. Splitted Data

**Step 4** : L is a set of buffers that have a nid, and we can get L. Element of L is shown as Fig.e.

| Snid | Splitted Sequence Number | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| S1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| S2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| S3 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| S4 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| S5 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |

Fig.e. Final Secret Pieces

Through these step, every five member can share final secret pieces. Probably an important director will take S1 and S2 that have more weight. Even if a participant loses secret pieces among S3,S4,S5 for same reason, they can reconstruct original data with 100 percent probability.

4.3 Data Reconstruction scenario

Reconstruction is much simpler than splitting. w-table is required for reconstruction of the secrets. w-table is similar to the key that is used for encryption. If anyone who wants the recovery doesn't have w-table, he will never be able to reconstruct the original data.

For secret recovery, the reconstructor named Sally collects w-table and secret pieces as shown in Fig.f. Suppose Sally collects secret piece S1 to S4 except S5.

| Snid | Splitted Sequence Number | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| S1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| S2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| S3 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| S4 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |

Fig.f Collected Secret Pieces

Sally will reconstruct the original data by using collected data.

**Step 1** : Calculate buffer size for reconstruction.

Sally can calculate buffer size b as follows.

$$b \leftarrow \sum_{nid=1}^{k} W_{nid} = 3+2+1+1 = 7$$

For reconstruction, buffers are created as in Fig.g.

| B1 | B2 | B3 | B4 | B5 | B6 | B7 |
|---|---|---|---|---|---|---|
| S1 | S1 | S1 | S2 | S2 | S3 | S4 |

Fig.g. Created Buffers For Reconstruction

**Step 2** : Sally can get the original data by multiplying elements by weight and compare to $\frac{b}{2}$.

The original data is

$$\begin{cases} 1 \text{ if } \frac{b}{2} \le \sum_{nid=1}^{k} W_{nid} S_{nid} \\ 0 \ otherwise \end{cases}$$

For example, First value(splitted sequence

number 1) of original data is 1 as a result of comparing the calculation

$(3\times0)+(2\times1)+(1\times1)+(1\times1) = 4$ with $\frac{7}{2}$.

All of the final reconstructed data are shown as in Fig.h.

| Bbid | Snid | Splitted Sequence Number | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| B1 | S1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| B2 | S1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| B3 | S1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| B4 | S2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| B5 | S2 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| B6 | S3 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| B7 | S4 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |

Reconstruction

| Binary Data | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Fig.h. Final Reconstructed Data

Let us examine the security about secret pieces when reconstructing the original data.

if the reconstructor does not collects w-table, he can't analogize the original data, and consequently, can keep it confidential.
For example, suppose that an malicious attacker collects all secret piece, but he makes an arbitrary prediction about w-table. The following is the w-table predicted by the attacker.

Table b. w-table predicted by attacker

| Description | nid | Weight |
|---|---|---|
| Secret Piece A | 1 | 1 |
| Secret Piece B | 2 | 3 |
| Secret Piece C | 3 | 2 |
| Secret Piece D | 4 | 1 |
| Secret Piece E | 5 | 1 |

If prediction first value(splitted sequence number 1) of original data in Fig. e using Table d,

$\frac{8}{2} > \sum_{nid=1}^{k} S_{nid}$ i.e., Result value is predicted 0 by 4 = 4.

Accordingly, the attacker will get quite different number of data bit 1.
The attacker will get 1101000001110 that is quite different from what is obtainable from the repetition of the reconstruction procedures.

Therefore, The final data is created as something like 6670, which is quite a different number from binary operation of 1101000001110.

In case of encrypt 0 and 1 in the binary number, we can possibly decrypt original data by probability of $\frac{1}{2}$ = 0.5.

But, the size of binary data is n, decryption probability is decrease to $\frac{1}{2^n}$.

i.e., In our example, decryption probability is $\frac{1}{2^{13}}$ because the size of binary number is 13.
This case, Return to original data is a very hard problem.

**Step 3** : Sally can reconstruct original data by conversion of final binary data.
I.e., Sally get 7342 by decimal calculation of binary data that is 1110010101110.

## V. Analysis

This section is devoted to analyzing the efficiency of our scheme comparing to existing schemes.

The online secret sharing protocol of C.Cachin can reconstruct multiple secrets through information Tx and X, but it was

Table c. Efficiency of analysis in our scheme

| Description | Number of Parameter | Addition | Multiplication | Modulo Exponent | Hash |
|---|---|---|---|---|---|
| Cachin's Scheme | 2 | k+1 | - | 1 | 1 |
| Pinch's Scheme | 3 | k | - | $2k^2+1$ | k |
| Ghodosi's Scheme | 4 | 1 | - | k | 1 |
| Our Scheme | 2 | k | k | - | - |

required distributed computation for recovery of more than one piece of information.

To supplement this, Pinch proposes Diffie-Hellman and a one-way function based on protocol named online multiple secret sharing protocol, but Pinch's scheme has a limitation that it requires a large capacity calculation because of *modulo exponent* operation.

On the other hand, Godoshi modified Pinch's scheme, but it still has the same as Pinch's scheme has problem.

Also, the problem with management of privacy data using traditional proposed scheme arises.
The scheme proposed in this paper makes the simple and rapid reconstruction of the original data possible, through k-time multiplication and k-time addition operation for the purpose of the reconstruction of $L_k$ and w-table.

## VI. Conclusion

Due to the influx of ubiquitous computing, the range of privacy data has increased dynamically.
Enterprises need to collect and manage such dynamic privacy data to facilitate their business.
To establish secure ubiquitous environment, the protection of privacy data must be required.
This suggests that we need the technology of privacy data management that is suitable for ubiquitous computing environment.

We discuss secret sharing scheme for privacy data management.
But, the existing secret sharing scheme are not suitable for the management of large a quantity of data because that required operation of large capacity.
Besides, the existing scheme not considering the weight of secret pieces was not able to manage the privacy data .

In this paper, We propose new secret sharing scheme for privacy data management. Our scheme makes high-speed operation possible, and it also allows for set weight for each secret pieces depending on weight of participants.

The scheme proposed in this paper makes it efficient to collect and manage secure privacy data in ubiquitous environment.

## [References]

[1] C.Cachin, "On-line Secret Sharing", Cryptography and Coding, LNCS 1025 190-198, 1995
[2] Borko Furht, "An Innovative Internet Architecture for Application Service Providers", Proceedings of the 33 rd Hawaii International Conference on System Sciences,

2000
[3] H. Ghodosi, et al. "How to prevent cheating in Pinch's scheme", Electronics Letters, Volume 33, Issue 17, p. 1453-1454, 1997
[4] R.G.E. Pinch, "Online Multiple Secret Sharing", Electronics Letters, 1996
[5] A.Shamir, "How to share a secret", Communications of the ACM, 1979
[6] O. Goldreich, et al., " How to play ANY mental game ", ACM, Proceedings of the nineteenth annual ACM conference on Theory of computing, pp.218-229, 1987
[7] G.R. Blakely, "Safeguarding cryptographic key", Proceedings of AFIPS National Computer Conference, pp.313-317, 1979
[8] W.Diffe, M.Hellman, "New Directions in Cryptography", IEEE Transaction on Information Theory, pp.644-654, 1976
[9] Chan Yeob Yeun, et al. "How to identify all cheater in Pinch's Scheme", Japan-Singapole Joint Workshop on Information Security, 1998.
[10] J.He, et al., "Multisecret-sharing scheme based on one-way function", Electronic letters, Vol.31 No.2, 1995