

# Stochastic Protection of Confidential Information in Databases: A Hybrid of Data Perturbation and Query Restriction

## Online Supplement: Expository Example

Manuel A. Nunez, Robert S. Garfinkel, and Ram D. Gopal

School of Business, University of Connecticut, 2100 Hillside Road, Storrs, Connecticut 06269, mnunez@business.uconn.edu,  
rgarfinkel@business.uconn.edu, ram@business.uconn.edu

### 1. Input Data

We illustrate the proposed approach with an expository example. Consider the database given in Table 1 with two confidential attributes: income and credit. Let  $a_i$  and  $b_i$  denote the values of income and credit for record  $i$ . Consider the target set  $T$  consisting of the following queries.

$$\begin{aligned}
 q_1(a, b) &:= a_1 + a_2 + a_3 + a_4, \\
 q_2(a, b) &:= b_1 + b_2 + b_3 + b_4, \\
 q_3(a, b) &:= b_1 + b_2 + b_3, \\
 q_4(a, b) &:= a_1 + a_3 + a_4 + a_5 + a_6, \\
 q_5(a, b) &:= \min\{a_1, a_2, a_3, a_4\}, \\
 q_6(a, b) &:= \min\{b_1, b_2, b_3, b_4\}, \\
 q_7(a, b) &:= a_1 + a_2, \\
 q_8(a, b) &:= (a_1 + a_2)(a_1 - a_2), \\
 q_9(a, b) &:= \text{var}(a_1, a_2), \\
 q_{10}(a, b) &:= \text{corr}(a, b).
 \end{aligned}$$

Note that income and credit attributes are correlated (correlation coefficient of 0.478). The query  $q_{10}$  indicates that the Database Manager (DBM) would like to disseminate the correlation between the two confidential attributes. The weights on all the queries are assumed identical, although if answering the correlation query exactly were a strict requirement, it could clearly be given a weight larger than the sum of all other queries. The stochastic protection requirements are set as follows.

$$\text{Income : } \Pr\{a_i \in [r, s]\} \leq 1/45, \forall i = 1, \dots, 6, s - r = 1;$$

**Table 1** Original Data.

Record	Income	Credit
1	97	78
2	78	37
3	79	80
4	29	45
5	75	70
6	61	75

**Table 2** Perturbed Data.

Record	Income	Credit
1	60.1	37
2	114.9	94
3	29	72
4	79	37
5	67.9	95.9
6	105	122.6

$$\text{Credit} : \Pr \{b_i \in [r, s]\} \leq 1/80, \forall i = 1, \dots, 6, s - r = 1.$$

## 2. Design Phase 1: Exact Answers

The objective in the first phase is to obtain the maximum number of queries from the target set  $T$  that can be answered exactly, while satisfying the stochastic protection requirements set by the DBM. This problem is solved in two steps.

In the first step, algorithm MIG is employed to obtain a subset of  $T$  such that the confidential information of all the subjects is protected from exact disclosure, where disclosure occurs by users linearly combining queries to infer confidential data. When applied to the above 10 queries, algorithm MIG yields either one of the following two sets of queries:

$$\begin{aligned} S_1 &:= \{q_1, q_2, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\} = T \setminus \{q_3\}; \\ S_2 &:= \{q_1, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\} = T \setminus \{q_2\}. \end{aligned}$$

Note that queries  $q_2$  and  $q_3$  cannot both be answered, since users can linearly combine the two queries to infer the credit score for record 4. Note further that queries  $q_7$ ,  $q_8$ , and  $q_9$  would all be answered at this stage. While confidential data is not disclosed through a linear combination of those queries, it is easy to see that answering any two of those three queries immediately yields the income values of records 1 and 2. This follows since answering  $q_7$  allows the user to determine that  $a_1 = 175 - a_2$ , which can then be used to solve for  $a_2$  from either the answer to  $q_8$  or  $q_9$ . Similarly, consider answering  $q_8$  and  $q_9$ . Since the answer to  $q_9$  can be written as  $(a_1 - a_2)^2/4 = 90.25$ , the magnitude of  $a_1 - a_2$  is known to be 19. Then since the answer to  $q_8$  is positive it must be that  $a_1 - a_2 = 19$ . Then, from  $q_8$ ,  $a_1 + a_2 = 175$ , so that  $a_1$  and  $a_2$  are exactly determined.

The objective of the second step is to further refine the chosen set of queries to ensure that all records are stochastically protected, and that this level of protection cannot be circumvented by any inference scheme. The algorithm described in Section 3 of the paper is employed on the above the query set  $S_1$ . The resulting set of queries for which exact answers can be provided is the following.

$$S_3 = \{q_1, q_2, q_4, q_5, q_6, q_7, q_{10}\} = T \setminus \{q_3, q_8, q_9\}.$$

## 3. Design Phase 2: Consistent Perturbation

In the second design phase a perturbation vector for income and credit attributes is developed. Note that the perturbed data is consistent with the exact answers of the queries in  $S_3$  and also offers stochastic protection. The perturbed data is shown in Table 2.

## 4. Run Time Stage

At the completion of the design stage, both exact answers to queries in  $S_3$  and the perturbed database are made public. The users can pose any query on the database. User answers are provided as follows:

- The user query is computed on the perturbed database.
- If the query is in  $S_3$ , then the user is informed that the answer is exact.

**Table 3** Run Time Queries.

Query	Perturbed Answer/ Guaranteed Exact?	Exact Answer	Similar ‘Altered’ Queries
$a_1 + a_2 + a_3$	204 / No	254	$a_1 + a_2 + a_3 + a_4$ $a_1 + a_2$ $a_3 + a_4$
$\frac{a_1 + a_2 + a_3 + a_4}{b_1 + b_2 + b_3 + b_4}$	1.179 / Yes	1.179	None
$\max \{a_1, a_2, a_3, a_4\}$	114.9 / No	97	$\min \{a_1, a_2, a_3, a_4\}$ $a_1 + a_2$ $a_3 + a_4$

• Optionally, if an exact answer to the original user cannot be provided, an exact answer to one or more queries that are ‘slightly altered’ from the user query can be provided. Many measures of the degree of alteration of a query could be considered. The most natural would be that, if possible, the functional form of the altered query would be the same as that requested. Then a secondary objective would be that the support sets of the two queries be as close as possible, where “closeness” would best be measured from an application point of view. For instance, as indicated earlier, the support set corresponding to professors in a given department may be deemed “close” to that of professors in one of two related departments. Lacking such a specific application, here we illustrate closeness based simply on the similarity of the index sets. Finally it may also be possible to guarantee that the requested query can be answered exactly if it is seen to be any combination of the queries in the set  $S_3$ .

This is illustrated in Table 3 with a sample of queries.