Assessing the disclosure risk of CTA-like methods

Jordi Castro
jordi.castro@upc.edu
Dept. of Statistics and Operations Research
Universitat Politècnica de Catalunya
Barcelona

This work has been supported by grants MTM2012-31440 of the Spanish research program and SGR-2009-1122 of the Government of Catalonia
Contents

1. Introduction
2. Outline of minimum distance CTA
3. Attacker scenarios considered
4. Computational results
Motivation I

Tabular protection method: map $F : Tables \rightarrow Tables$ such that $F(T) = T'$ and $T'$ is “safe”.

"safe": tight estimates of sensitive cells can not be recomputed. Therefore, the inverse map $T' = F^{-1}(T)$ should not be available or difficult to compute by any attacker, otherwise disclosure risk is high.

CTA: post-tabular approach which looks for safe table $T'$ closest to original $T$. It solves a minimum-distance optimization problem. CTA-like methods have low disclosure risk if no attacker can obtain $\hat{T} = \hat{F}^{-1}(T')$, $\hat{F}^{-1}$ being an estimate of $F^{-1}$.
Motivation I

- Tabular protection method: map $F : \text{Tables} \rightarrow \text{Tables}$ such that $F(T) = T'$ and $T'$ is “safe”.

- “safe”: tight estimates of sensitive cells can not be recomputed.
Motivation I

- Tabular protection method: map $F : \text{Tables} \rightarrow \text{Tables}$ such that $F(T) = T'$ and $T'$ is “safe”.

- “safe”: tight estimates of sensitive cells can not be recomputed.

- Therefore, the inverse map $T = F^{-1}(T')$ should not be available or difficult to compute by any attacker, otherwise disclosure risk is high.
Motivation I

- Tabular protection method: map $F : \text{Tables} \rightarrow \text{Tables}$ such that $F(T) = T'$ and $T'$ is “safe”.
- “safe”: tight estimates of sensitive cells cannot be recomputed.
- Therefore, the inverse map $T = F^{-1}(T')$ should not be available or difficult to compute by any attacker, otherwise disclosure risk is high.
- CTA: post-tabular approach which looks for safe table $T'$ closest to original $T$. It solves a minimum-distance optimization problem.
Motivation I

- Tabular protection method: map $F : \text{Tables} \rightarrow \text{Tables}$ such that $F(T) = T'$ and $T'$ is “safe”.

- “safe”: tight estimates of sensitive cells can not be recomputed.

- Therefore, the inverse map $T = F^{-1}(T')$ should not be available or difficult to compute by any attacker, otherwise disclosure risk is high.

- CTA: post-tabular approach which looks for safe table $T'$ closest to original $T$. It solves a minimum-distance optimization problem.

- CTA-like methods have low disclosure risk if no attacker can obtain a good estimate $\hat{T} = \hat{F}^{-1}(T')$, $\hat{F}^{-1}$ being an estimate of $F^{-1}$. 
Motivation II

This talk:

- considers 4 different attacker scenarios;
This talk:

- considers 4 different attacker scenarios;
- provides exhaustive empirical evaluation of the disclosure risk of CTA;

(UNECE, Ottawa, October 28–30, 2013)
This talk:

- considers 4 different attacker scenarios;
- provides exhaustive empirical evaluation of the disclosure risk of CTA;
- reports results for the solution of more than 2500 optimization attacker problems;

Summary:

This talk:

- considers 4 different attacker scenarios;
- provides exhaustive empirical evaluation of the disclosure risk of CTA;
- reports results for the solution of more than 2500 optimization attacker problems;
- summarizes results in the paper: 
Contents

1 Introduction

2 Outline of minimum distance CTA

3 Attacker scenarios considered

4 Computational results
CTA: Example

**ORIGINAL TABLE. Protection levels:** $x_{23} \geq 45$ or $x_{23} \leq 35$

<table>
<thead>
<tr>
<th></th>
<th>$Z_1$</th>
<th>$Z_2$</th>
<th>$Z_3$</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_1$</td>
<td>20</td>
<td>24</td>
<td>28</td>
<td>72</td>
</tr>
<tr>
<td>$E_2$</td>
<td>38</td>
<td>38</td>
<td>40</td>
<td>116</td>
</tr>
<tr>
<td>$E_3$</td>
<td>40</td>
<td>39</td>
<td>42</td>
<td>121</td>
</tr>
<tr>
<td>TOTAL</td>
<td>98</td>
<td>101</td>
<td>110</td>
<td>309</td>
</tr>
</tbody>
</table>
**CTA: Example**

**ORIGINAL TABLE.** Protection levels: $x_{23} \geq 45$ or $x_{23} \leq 35$

<table>
<thead>
<tr>
<th></th>
<th>$Z_1$</th>
<th>$Z_2$</th>
<th>$Z_3$</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_1$</td>
<td>20</td>
<td>24</td>
<td>28</td>
<td>72</td>
</tr>
<tr>
<td>$E_2$</td>
<td>38</td>
<td>38</td>
<td>40</td>
<td>116</td>
</tr>
<tr>
<td>$E_3$</td>
<td>40</td>
<td>39</td>
<td>42</td>
<td>121</td>
</tr>
<tr>
<td>TOTAL</td>
<td>98</td>
<td>101</td>
<td>110</td>
<td>309</td>
</tr>
</tbody>
</table>

**PROTECTED TABLE:** either ... or ...

<table>
<thead>
<tr>
<th></th>
<th>$Z_1$</th>
<th>$Z_2$</th>
<th>$Z_3$</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_1$</td>
<td>25</td>
<td>24</td>
<td>23</td>
<td>72</td>
</tr>
<tr>
<td>$E_2$</td>
<td>33</td>
<td>38</td>
<td>45</td>
<td>116</td>
</tr>
<tr>
<td>$E_3$</td>
<td>40</td>
<td>39</td>
<td>42</td>
<td>121</td>
</tr>
<tr>
<td>TOTAL</td>
<td>98</td>
<td>101</td>
<td>110</td>
<td>309</td>
</tr>
</tbody>
</table>

(UNECE, Ottawa, October 28–30, 2013)
General formulation of CTA

- Set of cells $a_i, i = 1, \ldots, n$.
- Set $S = \{i_1, i_2, \ldots, i_s\} \subseteq \{1, \ldots, n\}$ of indices of sensitive cells.
- Linear relations $Aa = b$.
- Lower and upper protection level for each sensitive cell $i \in S$: $lpl_i$ and $upl_i$.
- Lower and upper bound for each cell: $l_{a_i}$ and $u_{a_i}$.
- Cell weights $w_i$ for cost of adjustment of each cell.
General formulation of CTA

- Set of cells $a_i, i = 1, \ldots, n$.
- Set $S = \{i_1, i_2, \ldots, i_s\} \subseteq \{1, \ldots, n\}$ of indices of sensitive cells.
- Linear relations $Aa = b$.
- Lower and upper protection level for each sensitive cell $i \in S$: $lpl_i$ and $upl_i$.
- Lower and upper bound for each cell: $l_{a_i}$ and $u_{a_i}$.
- Cell weights $w_i$ for cost of adjustment of each cell.

CTA formulation:

$$\min_{x} \|x - a\|_{\ell(w)}$$

s. to

$$Ax = b$$

$$l_{a_i} \leq x_i \leq u_{a_i} \quad i \in N$$

$$(x_i \leq a_i - l_{pl_i}) \text{ or } (x_i \geq a_i + u_{pl_i}) \quad i \in S.$$
CTA formulation fixing protection senses

- Defining $z = x - a$, and fixing the protection senses we have the convex problem:
  \[
  \min_z \|z\|_{\ell(w)} \\
  \text{s. to } Az = 0 \\
  l(a) \leq z \leq u(a),
  \]

- For $\ell_1$ norm we have the linear problem
  \[
  \min_{z^+,z^-} \sum_{i=1}^n w_i(a_i)(z_i^+ + z_i^-) \\
  \text{s. to } A(z^+ - z^-) = 0 \\
  l^+(a) \leq z^+ \leq u^+(a) \\
  l^-(a) \leq z^- \leq u^-(a),
  \]

- For $\ell_2$ norm we have the convex quadratic problem
  \[
  \min_z \sum_{i=1}^n w_i(a_i)z_i^2 \\
  \text{s. to } Az = 0 \\
  l(a) \leq z \leq u(a).
  \]
Contents

1. Introduction
2. Outline of minimum distance CTA
3. Attacker scenarios considered
4. Computational results
Attacker scenarios considered

**Attacker information and attacker problem**

Attacker wants to obtain a *good* estimate \( \hat{z} \) of \( z \) from released \( T' \).

- **Attacker complete information:**
  - Released values \( x \).
  - Structure of the table, i.e., constraints matrix \( A \).

- **Attacker partial information:**
  - Distance used.
  - Cell weights \( w(a) \): depend on function of \( a \)
  - Bounds \( l^+(a), l^-(a), u^+(a), u^-(a), u(a), l(a) \): depend on \( a, S \) and protection senses.

**Optimization problem to be solved by attacker**

\[
\begin{align*}
\text{min} & \quad ||\hat{Z}||_{\ell(x)} \\
\text{s. to} & \quad A\hat{Z} = 0 \\
& \quad \hat{l}(x) \leq \hat{z} \leq \hat{u}(x)
\end{align*}
\]

where \( \hat{l}(x) \) and \( \hat{u}(x) \) are estimates of the bounds.
Attacker scenarios considered

B. The attacker has incomplete information about both the bounds and objective function, but he/she knows the subset $S$ of sensitive cells, and the original cell bounds $l_{a_i}$ and $u_{a_i}$, $i \in \mathcal{N}$ (which are quite strong assumptions). We have three subscenarios:

B1. The attacker neither knows the protection levels $upl_i$, $lpl_i$, $i \in S$, nor the protection sense.

B2. The attacker knows the protection sense, but not the protection levels $upl_i$, $lpl_i$, $i \in S$.

B3. The attacker knows both the protection sense and protection levels $upl_i$, $lpl_i$, $i \in S$. The only unknown terms to reproduce the real bounds are then $a_i - l_{a_i}$ and $u_{a_i} - a_i$, $i \in \mathcal{N}$.

C. The attacker has complete information about the bounds, i.e., he/she knows all the parameters but the objective function $w$. 
Computational results

Contents

1. Introduction
2. Outline of minimum distance CTA
3. Attacker scenarios considered
4. Computational results
33 standard instances from the literature.

Procedure:

- Tables first protected with $\ell_1$-CTA and $\ell_2$-CTA.
- Next, attacker problems solved for the four scenarios, 10 random replications for different values of $\tilde{x}$.

This amounts to: 33 instances $\times$ 2 distances $\times$ 4 scenarios $\times$ 10 replications = 2640 optimization problems.

Following plots show the distribution of percentage differences between estimates and true values of sensitive cells $|\hat{a}_i - a_i|/a_i \cdot 100$, $i \in S$ for all the attacker problems, and the different scenarios.
Results for scenario B1

CTA is safe for scenario B1

\( \ell_1 \) and \( \ell_2 \) are similar
Results for scenario B2

\( \ell_1 \)  \hspace{1cm}  \ell_2

CTA is safe for scenario B2.

\( \ell_2 \) seems to be safer than \( \ell_1 \).
Results for scenario B3

\[
\ell_1 \\
\ell_2
\]

CTA is not safe for scenario B3

\( \ell_2 \) is safer than \( \ell_1 \)
Results for scenario C

CTA is not safe for scenario C

$\ell_2$ is safer than $\ell_1$
Conclusions

- Scenarios B1 and B2 are safe. The estimate $\hat{a}_i$ was never equal to the true cell value $a_i$, and the distribution is not concentrated on the left intervals.
Conclusions

- Scenarios B1 and B2 are safe. The estimate $\hat{a}_i$ was never equal to the true cell value $a_i$, and the distribution is not concentrated on the left intervals.

- For scenarios B3 and C the attacker was able to re-compute in almost 100% of the cases the original values $a$. 

$\ell_2$ seems to reduce more than $\ell_1$ the disclosure risk: the distribution is more left-skewed for $\ell_2$ in scenarios B1 and B2.

Conclusion: CTA is safe, unless the attacker has good information about the protection levels, protection senses, set of sensitive cells, and lower and upper bounds. However the knowledge of such big amount of information by the attacker may be a strong assumption.
Scenarios B1 and B2 are safe. The estimate $\hat{a}_i$ was never equal to the true cell value $a_i$, and the distribution is not concentrated on the left intervals.

For scenarios B3 and C the attacker was able to re-compute in almost 100% of the cases the original values $a$.

$l_2$ seems to reduce more than $l_1$ the disclosure risk: the distribution is more left-skewed for $l_2$ in scenarios B1 and B2.
Conclusions

- Scenarios B1 and B2 are safe. The estimate $\hat{a}_i$ was never equal to the true cell value $a_i$, and the distribution is not concentrated on the left intervals.

- For scenarios B3 and C the attacker was able to re-compute in almost 100% of the cases the original values $a$.

- $\ell_2$ seems to reduce more than $\ell_1$ the disclosure risk: the distribution is more left-skewed for $\ell_2$ in scenarios B1 and B2.

- Conclusion: CTA is safe, unless the attacker has good information about the protection levels, protection senses, set of sensitive cells, and lower and upper bounds. However the knowledge of such big amount of information by the attacker may be a strong assumption.
Thanks for your attention!