Suplementary Material

Zeyin Hou, Shuai Lu, Zhi Wu, Wei Gu, Hao Zhang, Yijun Xu, Zihang Gao

July 16, 2024

1 Privacy Analysis

In this section, we carry out the privacy analysis for the privacy-preserved computation method. Privacy is defined as the indoor temperature matrix $\boldsymbol{\tau}_{in}^{-m}$ ($\forall m \in \mathbf{M}$) the random matrix $\boldsymbol{W}$. It is worth mentioning that although $\boldsymbol{W}$ does not directly involve the private information of agents, the BLA can infer the $\boldsymbol{\tau}_{in}^{-m}$ by combining $\boldsymbol{\tau}_{in}^{-m}\boldsymbol{W}^\top$ and $\boldsymbol{W}$.

We need to analyze the information that BLA can potentially use to infer privacy. First, the BLA can aggregate the received information from agents, i.e., $\tilde{\boldsymbol{A}}_1^{-m,i}$ ($\forall m \in \mathbf{M}, \forall i \in \mathbf{K}$), $\tilde{\boldsymbol{A}}_2^i$ ($\forall i \in \mathbf{K}$) and $\tilde{\boldsymbol{A}}_3^i$ ($\forall i \in \mathbf{K}$), to get the aggregate information, i.e., $\boldsymbol{\tau}_{in}^{-m}\boldsymbol{W}^\top$ ($\forall m \in \mathbf{M}$), $\boldsymbol{W}\boldsymbol{W}^\top$ and $1^\top\boldsymbol{W}^\top$, to make privacy inference. Besides, the relationship between $\boldsymbol{\xi}$ and $\bar{\boldsymbol{\xi}}$, i.e., $\boldsymbol{\xi} = \boldsymbol{W}\bar{\boldsymbol{\xi}}$ is also useful for privacy inference. For convenience, we divide them into two categories, i.e., only $\boldsymbol{W}$-related information, and $\{\boldsymbol{\tau}, \boldsymbol{W}\}$-related information. We denote $\boldsymbol{W}\boldsymbol{W}^\top$ as $\boldsymbol{D}_1 \in \mathbb{R}^{K\times K}$, $1^\top\boldsymbol{W}^\top$ as $\boldsymbol{d}_1 \in \mathbb{R}^{K\times 1}$, $\boldsymbol{\tau}_{in}^{-m}\boldsymbol{W}^\top$ as $\boldsymbol{D}_2 \in \mathbb{R}^{T\times K}$. Then, we can define the two types of information as follows:

1) Type-1 information: only $\boldsymbol{W}$-related information ($\boldsymbol{W}$ is the matrix to be inferred)

$$\mathrm{I}_{\boldsymbol{W}} \triangleq \{\boldsymbol{W} | \boldsymbol{W}\boldsymbol{W}^\top = \boldsymbol{D}_1, 1^\top\boldsymbol{W}^\top = \boldsymbol{d}_1, \boldsymbol{W}^\top\bar{\boldsymbol{\xi}} = \boldsymbol{\xi}\} \tag{1a}$$

2) Type-2 information: $\{\boldsymbol{\tau}, \boldsymbol{W}\}$-related information ($\boldsymbol{\tau}_{in}^{-m}$ and $\boldsymbol{W}$ are the matrices to be inferred)

$$\mathrm{I}_{\boldsymbol{\tau},\boldsymbol{W}} \triangleq \{\boldsymbol{\tau}_{in}^{-m}\boldsymbol{W}^\top = \boldsymbol{D}_2\} \tag{1b}$$

The type-1 information can be used to infer the random matrix $\boldsymbol{W}$, while the type-2 information involves both $\boldsymbol{\tau}_{in}^{-m}$ and $\boldsymbol{W}$. In the following, we will carry out a detailed privacy analysis.

First, we analyze the possibility of the BLA inferring private information from the type-1 information. Based on the definition of type-1 information, the BLA can get the inference equations as follows:

$$\boldsymbol{W}\boldsymbol{W}^\top = \boldsymbol{D}_1, \tag{2a}$$

$$1^\top\boldsymbol{W}^\top = \boldsymbol{d}_1, \tag{2b}$$

$$\boldsymbol{W}^\top\bar{\boldsymbol{\xi}} = \boldsymbol{\xi}, \tag{2c}$$

wherein the the random matrix, $\boldsymbol{W}$, provides K^2 unknown variables. Note that the matrix, $\boldsymbol{D}_1$, is symmetric. Thus, (2a) provides $\sum_{i=1}^{K} i$, i.e, $\frac{K(K+1)}{2}$ independent inference equations. Besides, both (2b) and (2c) provide K inference equations. Overall, type-1 information has K^2 unknown variables and $\frac{K(K+1)}{2} + K + K = \frac{1}{2}K^2 + \frac{5}{2}K$ inference equations. When $K \geq 6$, the condition $K^2 > \frac{1}{2}K^2 + \frac{5}{2}K$ holds, which means the number of unknown variables is larger than the number of inference equations. Thus, the equation system is under-determined and the BLA cannot infer $\boldsymbol{W}$ when the condition $K \geq 6$ satisfies.

Second, we analyze the possibility of the BLA inferring private information from the type-2 information. Based on the definition of type-2 information, the BLA can get the inference equation as follows:

$$\boldsymbol{\tau}_{in}^{-m}\boldsymbol{W}^{\top} = \boldsymbol{D}_2, \quad \forall m \in \mathbf{M} \tag{3}$$

wherein $\boldsymbol{\tau}_{in}^{-m}$ ($\forall m \in \mathbf{M}$) and $\boldsymbol{W}$ provide $(T+M)K$ and K^2 unknown variables, respectively. (3) provides $(T+M)K$ inference equations. Considering the number of the unknown variables, i.e, $(T+M)K + K^2$, is larger than the number of the inference equations, i.e., $(T+M)K$, the equation system is under-determined and the BLA cannot infer the private information $\boldsymbol{W}$ or $\boldsymbol{\tau}_{in}^{-m}$.

Third, the BLA resorts to both the type-1 and type-2 information to implement privacy inference. The privacy inference equations can be formulated as:

$$\boldsymbol{W}\boldsymbol{W}^{\top} = \boldsymbol{D}_1, \tag{4a}$$

$$1^{\top}\boldsymbol{W}^{\top} = \boldsymbol{d}_1, \tag{4b}$$

$$\boldsymbol{W}^{\top}\bar{\boldsymbol{\xi}} = \boldsymbol{\xi}, \tag{4c}$$

$$\boldsymbol{\tau}_{in}^{-m}\boldsymbol{W}^{\top} = \boldsymbol{D}_2, \quad \forall m \in \mathbf{M} \tag{4d}$$

wherein $\boldsymbol{\tau}_{in}^{-m}$ and $\boldsymbol{W}$ provide $(T+M)K$ and K^2 unknown variables, respectively. On the other hand, (4a)-(4d) provide $\frac{K(K+1)}{2}$, K, K, and $(T+M)K$ inference equations, respectively. Similarly, when the number of unknown variables, i.e., $(T+M)K+K^2$ is larger than the number of inference equations, i.e., $\frac{K(K+1)}{2}+K+K+(T+M)K$, the equation system is under-determined. Through simple algebraic operations, we can conclude that when the condition $K \geq 6$ holds, the BLA cannot infer the private information.

In conclusion, when the number of agents satisfies $K \geq 6$, the BLA cannot infer the private information $\boldsymbol{\tau}_{in}^{-m}$ and $\boldsymbol{W}$, i.e., the privacy-preserved computation method is effective. It is worth mentioning that, the BLA is usually responsible for lots of multi-zone buildings (We assume each building zone is an agent in our paper). Thus, the condition $K \geq 6$ is satisfied in practical situations.